Rapidly improving Cybersecurity with a new global IdM/CKM design that does not rely on PKC

SLL's response to NIST's call

Presentation by
Benjamin Gittins (CTO)
Synaptic Laboratories Limited

Rapidly improving Cybersecurity with a new global IdM/CKM design that does not rely on PKC

SLL's response to NIST's call

We propose a method to scale Whitfield Diffie, Martin Hellman and Leslie Lamport's 1976 symmetric IdM/CKM proposal:

- to provision a wide range of high-availability cryptographic services
- that meets needs and priorities identified in NIST's 2009 CKM Workshop

Presentation by
Benjamin Gittins (CTO)
Synaptic Laboratories Limited

Table of Contents

Table of Contents

- Synaptic’s IdM/CKM project, architecture and design objectives
- Drivers for next generation CKM designs
  - from the NIST 2009 CKM Workshop
- Re-evaluating the original drivers that promoted PKD over SKD
  - Diffie et al (1976).
- The political treatise `Spirit of Laws’
  - a source of security design requirements
- Synaptic’s proposed architecture
  - high level overview
- The architectures techniques, cryptographic components, applications
  - a short survey
- Summary and call for collaborators!

Synaptic's Global IdM/CKM Project

Synaptic's Global IdM/CKM Project

In recognition that we live in a globally interdependent and interconnected information society

We are drawing together commercial and government collaborators for an international virtual Cluster of Excellence in Cybersecurity to complete design requirements, specifications and deployment of a global IdM/CKM

Synaptic's Global IdM/CKM Project

In recognition that we live in a globally interdependent and interconnected information society

We are drawing together commercial and government collaborators for an international virtual Cluster of Excellence in Cybersecurity to complete design requirements, specifications and deployment of a global IdM/CKM

Aiming for rapid international acceptance through:

1) international participation in the cluster

Synaptic's Global IdM/CKM Project

In recognition that we live in a globally interdependent and interconnected information society

We are drawing together commercial and government <u>collaborators</u> for an international virtual Cluster of Excellence in Cybersecurity to complete design requirements, specifications and deployment of a global IdM/CKM

Aiming for <u>rapid international acceptance</u> through:

1) international participation in the cluster
2) the use of existing NIST/FIPS security standards that are already trusted to achieve security against both classical and quantum computer attacks

Synaptic's Global IdM/CKM Project

In recognition that we live in a globally interdependent and interconnected information society

We are drawing together commercial and government collaborators for an international virtual Cluster of Excellence in Cybersecurity to complete design requirements, specifications and deployment of a global IdM/CKM

Aiming for rapid international acceptance through:

1) international participation in the cluster
2) the use of existing NIST/FIPS security standards that are already trusted to achieve security against both classical and quantum computer attacks
3) design decisions that ensure very low barriers to acceptance e.g. use existing hardware platforms, trusted ciphers, etc

Synaptic's IdM/CKM Architecture Objectives

Synaptic's IdM/CKM Architecture Objectives

To empower competitors and (semi-)autonomous authorities to work together, overcoming limitations of 'us versus them' fortress security paradigms

Synaptic's IdM/CKM Architecture Objectives

To empower competitors and (semi-)autonomous authorities to work together, overcoming limitations of 'us versus them' fortress security paradigms

Supporting Inter/intra domain co-operation - internationally

Synaptic’s IdM/CKM Architecture Objectives

To empower competitors and (semi-)autonomous authorities to work together, overcoming limitations of ‘us versus them’ fortress security paradigms

Supporting Inter/intra domain co-operation - internationally

To build an inclusive electronic IdM/CKM architecture that:

a) supports a thriving ecosystem of autonomous organisations working together to improve global security - increased assurance and trust

Synaptic's IdM/CKM Architecture Objectives

To empower competitors and (semi-)autonomous authorities to work together, overcoming limitations of 'us versus them' fortress security paradigms

Supporting Inter/intra domain co-operation - internationally

To build an inclusive electronic IdM/CKM architecture that:

a) supports a thriving ecosystem of autonomous organisations working together to improve global security - increased assurance and trust

b) enables ubiquitous encryption by reducing burdens on end users

Synaptic’s IdM/CKM Architecture Objectives

To empower competitors and (semi-)autonomous authorities to work together, overcoming limitations of ‘us versus them’ fortress security paradigms

Supporting Inter/intra domain co-operation - internationally

To build an inclusive electronic IdM/CKM architecture that:

a) supports a thriving ecosystem of autonomous organisations working together to improve global security - increased assurance and trust

b) enables ubiquitous encryption by reducing burdens on end users

c) rapidly improves cybersecurity - wraps around and protects current ICT and standards based security investments

Synaptic's IdM/CKM Architecture Objectives

To empower competitors and (semi-)autonomous authorities to work together, overcoming limitations of 'us versus them' fortress security paradigms

Supporting Inter/intra domain co-operation - internationally

To build an inclusive electronic IdM/CKM architecture that:

a) supports a thriving ecosystem of autonomous organisations working together to improve global security - increased assurance and trust

b) enables ubiquitous encryption by reducing burdens on end users

c) rapidly improves cybersecurity - wraps around and protects current ICT and standards based security investments

d) integrates with other cybersecurity initiatives such as network sensors

Synaptic’s IdM/CKM Design Objectives

Synaptic's IdM/CKM Design Objectives

1. IdM/CKM hosted in the cloud to service an international user base

Synaptic's IdM/CKM Design Objectives

1. IdM/CKM hosted in the cloud to service an international user base
2. Globally scalable architecture

Synaptic's IdM/CKM Design Objectives

1. IdM/CKM hosted in the cloud to service an international user base

2. Globally scalable architecture

3. Post quantum secure using NIST symmetric key techniques

Synaptic's IdM/CKM Design Objectives

1. IdM/CKM hosted in the cloud to service an international user base

2. Globally scalable architecture

3. Post quantum secure using NIST symmetric key techniques

4. Employs end-to-end redundancy to the user's token:

    5. Provide increased resilience against attacks by distributing trust across infrastructure

Synaptic's IdM/CKM Design Objectives

1. IdM/CKM hosted in the cloud to service an international user base

2. Globally scalable architecture

3. Post quantum secure using NIST symmetric key techniques

4. Employs end-to-end redundancy to the user's token:

    5. Provide increased resilience against attacks by distributing trust across infrastructure

6. User-centric design:

    7. Enable global key management/encryption by identifier: *a@b.com*

Synaptic's IdM/CKM Design Objectives

1. IdM/CKM hosted in the cloud to service an international user base

2. Globally scalable architecture

3. Post quantum secure using NIST symmetric key techniques

4. Employs end-to-end redundancy to the user's token:

    5. Provide increased resilience against attacks by distributing trust across infrastructure

6. User-centric design:

    7. Enable global key management/encryption by identifier: *a@b.com*

    8. Protect all legitimate stakeholder interests

Synaptic's IdM/CKM Design Objectives

1. IdM/CKM hosted in the cloud to service an international user base

2. Globally scalable architecture

3. Post quantum secure using NIST symmetric key techniques

4. Employs end-to-end redundancy to the user's token:

   5. Provide increased resilience against attacks by distributing trust across infrastructure

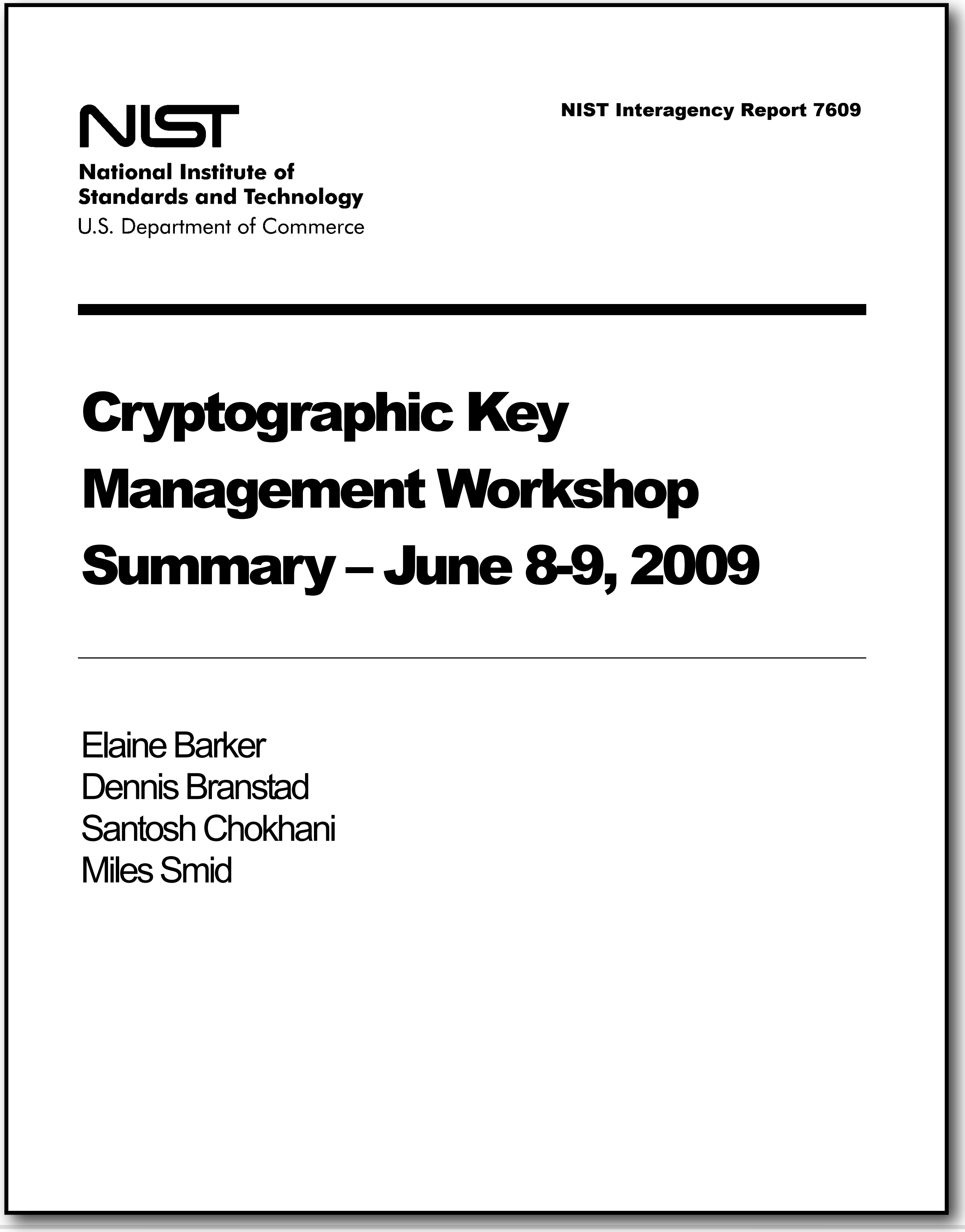
6. User-centric design:

   7. Enable global key management/encryption by identifier: *a@b.com*

   8. Protect all legitimate stakeholder interests

9. Protect existing PKI based security standards (SSL/TLS, SSH, IPsec, KMS...)

Rapidly improving Cybersecurity with a new global IdM/CKM design that does not rely on PKC; SLL's response to NIST's call



NIST

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Interagency Report 7609

Cryptographic Key Management Workshop Summary – June 8-9, 2009

Elaine Barker
Dennis Branstad
Santosh Chokhani
Miles Smid

2.4.6 Overall Summary of the CKM Workshop: Elaine Barker, NIST

(Note: Weather conditions caused the workshop to close early. This presentation was prepared but never presented. A summary of the presentation slides is included for completeness.)

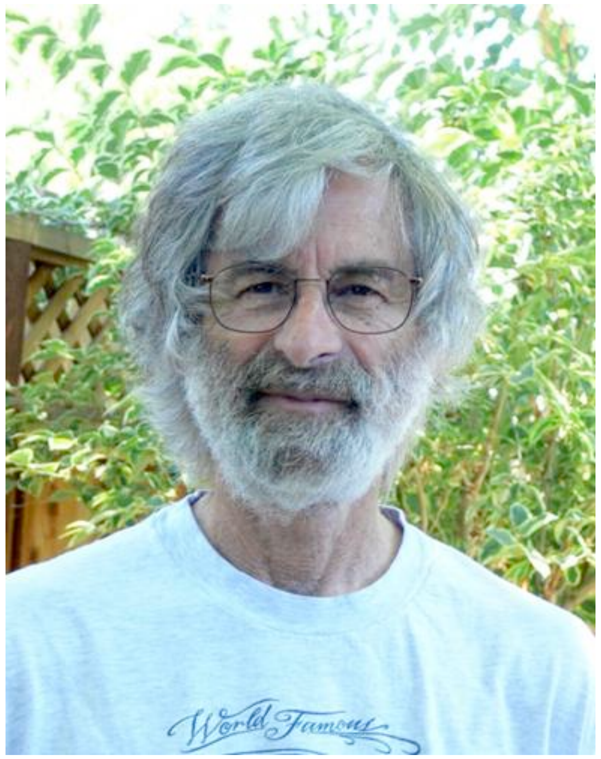
- Cryptographic Key Management: There is a major need to undertake key management as part of the national cybersecurity initiative. The CKM workshop is a first step towards a comprehensive and interoperable CKM. A joint government-industry partnership is the best approach.
- Considerations for future key management systems: Design systems for high availability and survivability. Prepare for emergency access to keys; worry about unintended consequences – both good and bad. In light of quantum computing, look at means other than using public keys. Look at quantum-resistant algorithms and schemes.
- Requirements for CKM: Must be user-friendly; easy to use – plug and play; must be a user-driven capability; must be secure, cost-effective, fault-tolerant, and highly available; must provide protection against destructive attacks and be interoperable; must be designed to be used enterprise-wide, by multi-partners that use multi-vendor products, and be usable by multi-applications; must be scalable and enhance interoperability in time of emergency. Metadata must be defined, as well as defining the security to protect it. We also need key inventory control, accountability/auditing of the keys, policies for managing the keys and metadata, and safety requirements for certain applications.

Re-evaluating the original drivers for PKC (Diffie et al)

W. Diffie

M. Hellman

R. Merkle



L. Lamport

Image of Diffie, Merkle: http://wikimedia

Image of Merkle: http://www.merkle.com/

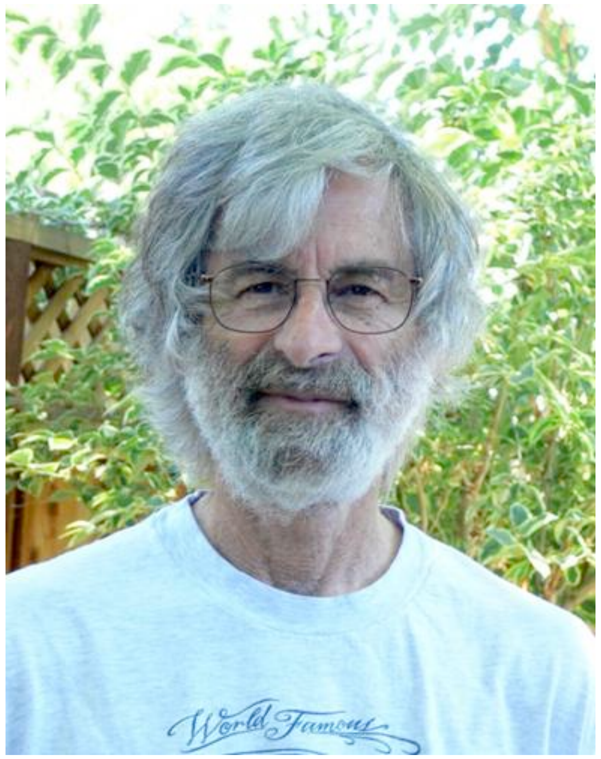
Image of Diffie, Merkle: http://research.microsoft.com/en-us/um/people/lamport/

Re-evaluating the original drivers for PKC (Diffie et al)

W. Diffie

M. Hellman

R. Merkle



L. Lamport

➠ The 4 Fathers of Public Key Cryptography

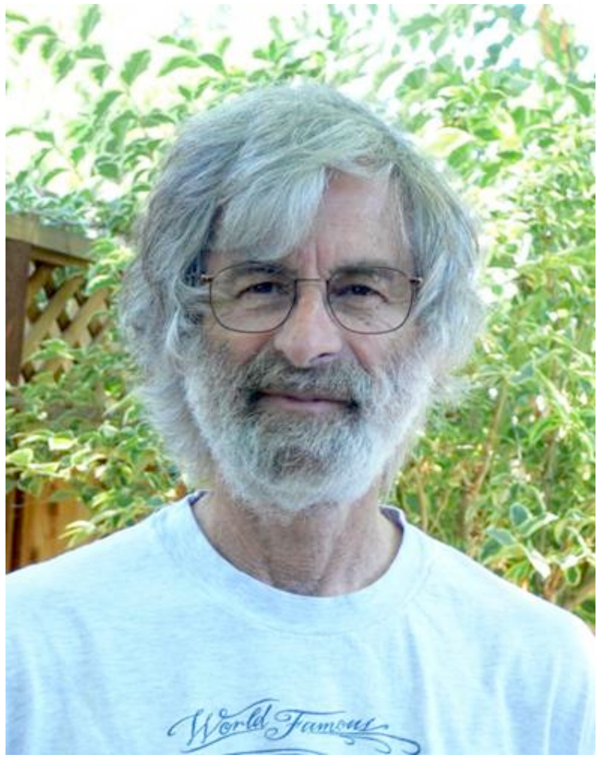
Image of Diffie, Merkle: http://wikimedia
Image of Merkle: http://www.merkle.com/
Image of Diffie, Merkle: http://research.microsoft.com/en-us/um/people/lamport/

Re-evaluating the original drivers for PKC (Diffie et al)

W. Diffie

M. Hellman

R. Merkle



L. Lamport

- The 4 Fathers of Public Key Cryptography
- Re-evaluating the 4 drivers that motivated Diffie-Hellman-Merkle to recommend Public Key Distribution over Symmetric Key Distribution

Image of Diffie, Merkle: http://wikimedia
Image of Merkle: http://www.merkle.com/
Image of Diffie, Merkle: http://research.microsoft.com/en-us/um/people/lamport/

Re-evaluating the original drivers for PKC (Diffie et al)

Re-evaluating the original drivers for PKC (Diffie et al)

➠ **Driver 1: Avoid the need for private key distribution channels**
(asymmetric designs do not use pre-shared secrets)

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 1: Avoid the need for <u>private</u> key distribution channels** (asymmetric designs do not use pre-shared secrets)
    - Success: <u>PKC</u> avoided online servers for **key exchange** operations

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 1: Avoid the need for private key distribution channels** (asymmetric designs do not use pre-shared secrets)
  - Success: PKC avoided online servers for **key exchange** operations
  - BUT: PKI needs **authenticated distribution** channels for distributing Root certificates **(identification)**

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 1: Avoid the need for private key distribution channels** (asymmetric designs do not use pre-shared secrets)
  - Success: PKC avoided online servers for **key exchange** operations
  - BUT: PKI needs **authenticated distribution** channels for distributing Root certificates **(identification)**

Background on smart card © Inmagine, Used with permission.

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 1: Avoid the need for private key distribution channels** (asymmetric designs do not use pre-shared secrets)
  - Success: PKC avoided online servers for **key exchange** operations
  - BUT: PKI needs **authenticated distribution** channels for distributing Root certificates **(identification)**
  - TODAY:

    CPU based smart cards can replace “trusted human couriers” for the private, tamper-evident, distribution of pre-shared symmetric keys

Background on smart card © Inmagine, Used with permission.

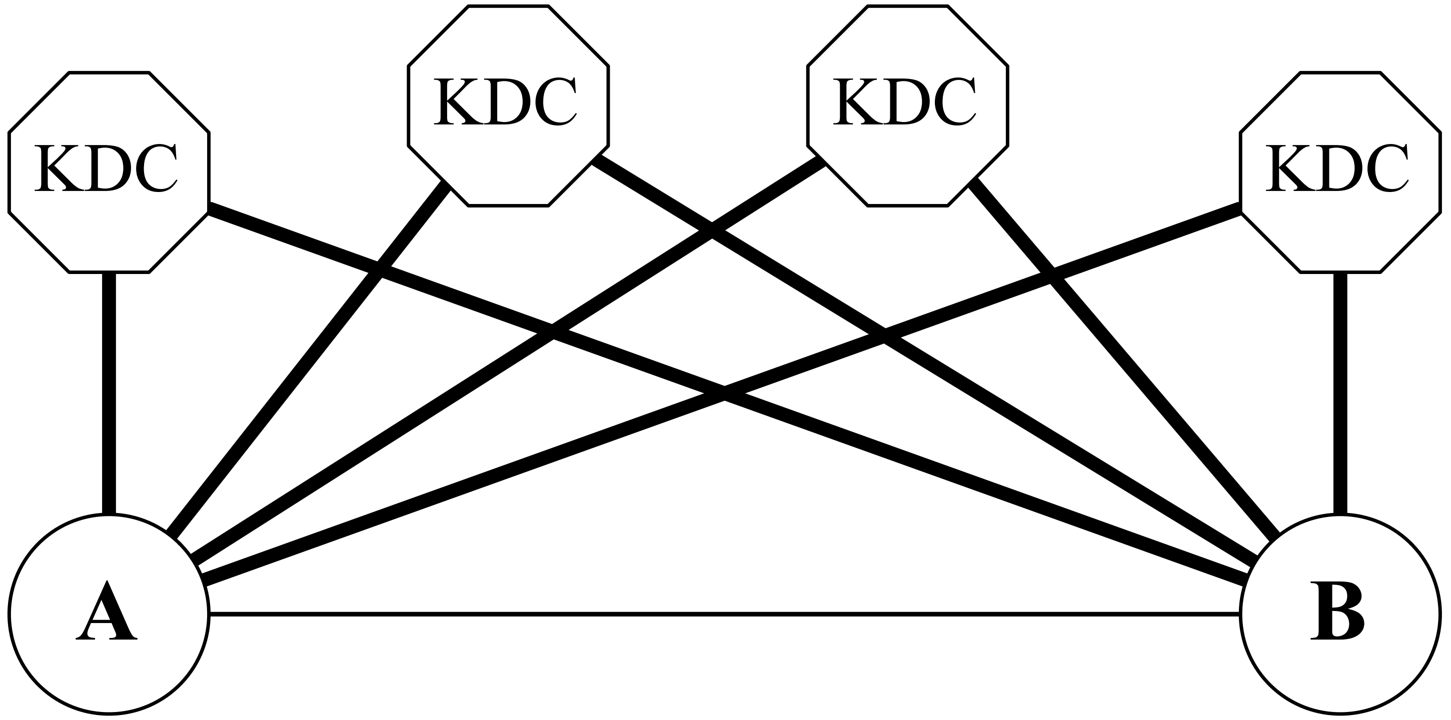
Re-evaluating the original drivers for PKC (Diffie et al)

Re-evaluating the original drivers for PKC (Diffie et al)

➠ **Driver 2: Enable private conversations between any two parties even if they have not communicated before**

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 2: Enable private conversations between any two parties even if they have not communicated before**
  - Diffie-Hellman-Lamport achieved this (1976) using SKD techniques

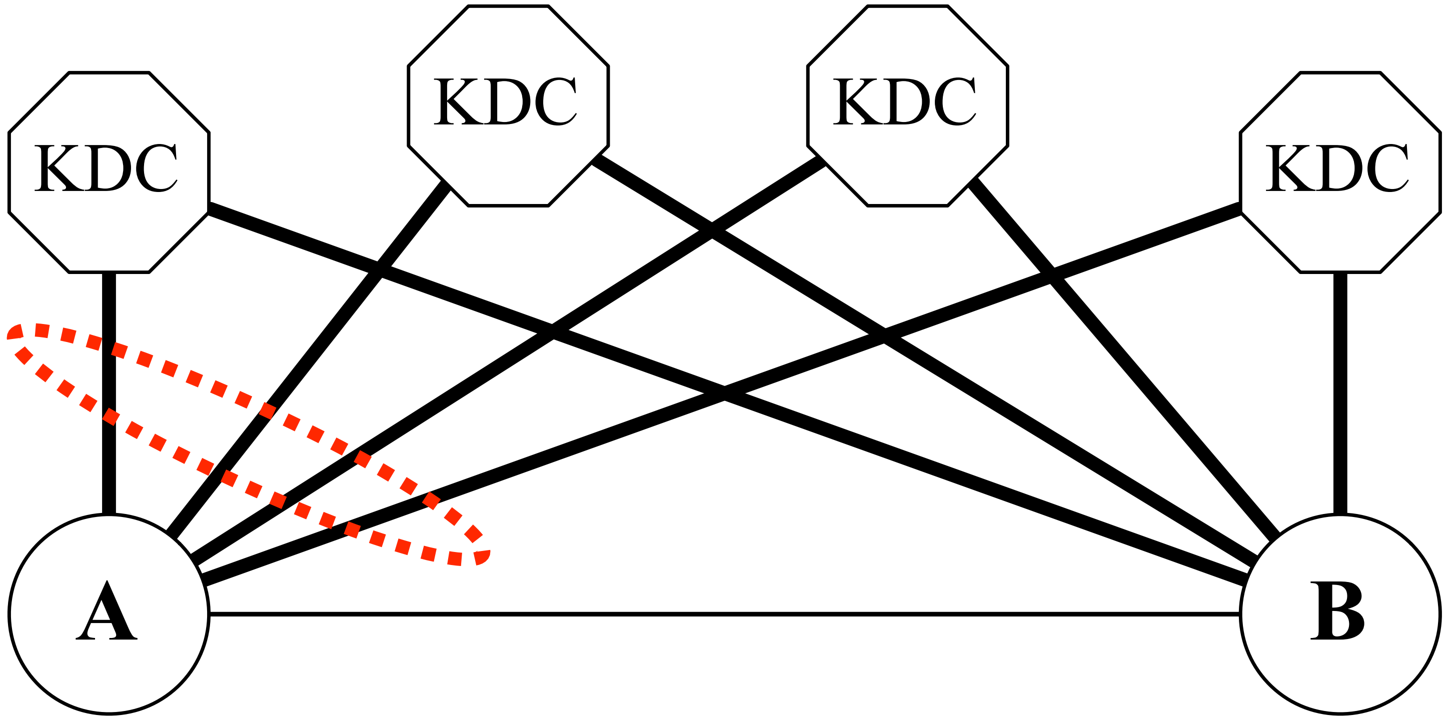


Key Distribution Center

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 2: Enable private conversations between any two parties even if they have not communicated before**
  - Diffie-Hellman-Lamport achieved this (1976) using SKD techniques
    - But it required low cost key distribution channels for *m* keys

***m* = 4 keys**

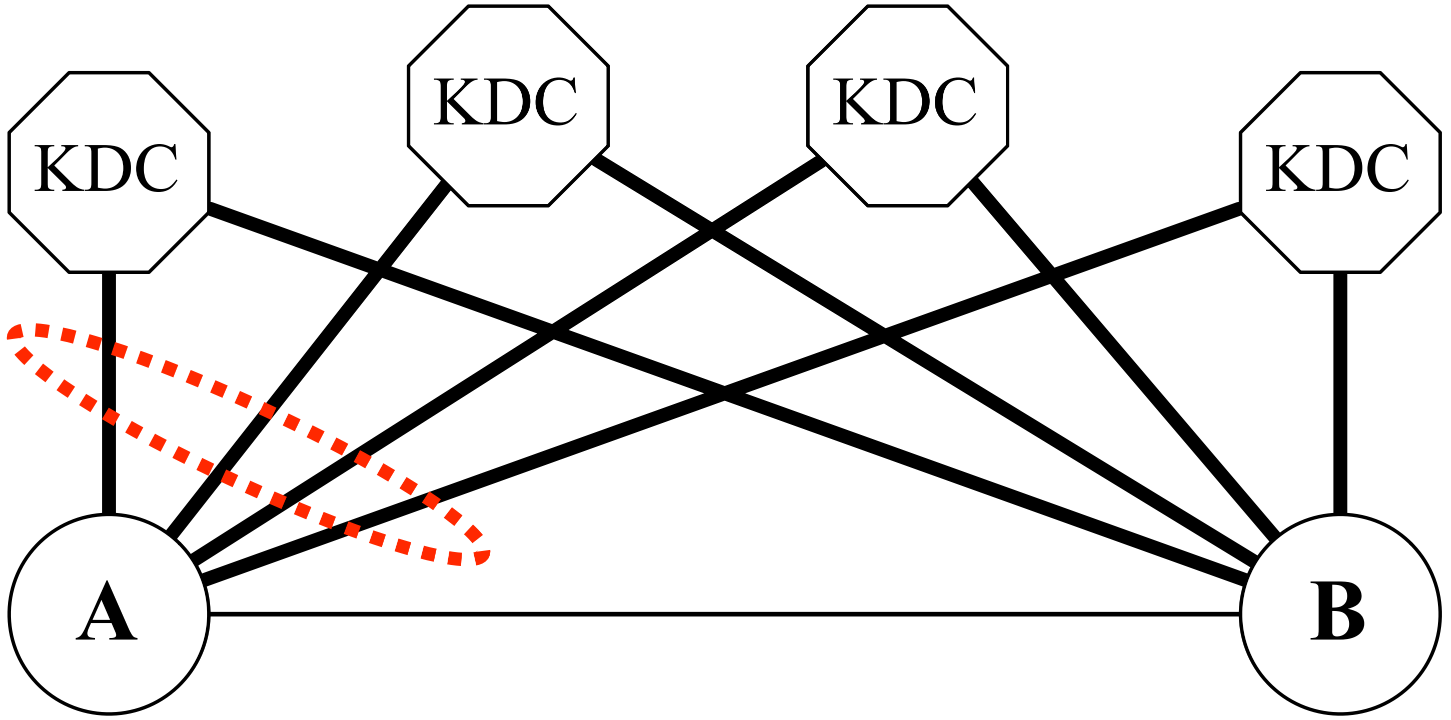


Key Distribution Center

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 2: Enable private conversations between any two parties even if they have not communicated before**
  - Diffie-Hellman-Lamport achieved this (1976) using SKD techniques
    - But it required low cost key distribution channels for *m* keys
    - PKD was selected (partly) due to SKD enrolment cost/scalability

m = 4 keys



Key Distribution Center

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 2: Enable private conversations between any two parties even if they have not communicated before**
  - Diffie-Hellman-Lamport achieved this (1976) using SKD techniques
    - But it required low cost key distribution channels for *m* keys
    - PKD was selected (partly) due to SKD enrolment cost/scalability

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 2: Enable private conversations between any two parties even if they have not communicated before**
  - Diffie-Hellman-Lamport achieved this (1976) using SKD techniques
    - But it required low cost key distribution channels for *m* keys
    - PKD was selected (partly) due to SKD enrolment cost/scalability
  - **TODAY:** Old barriers no longer apply
    - Networks are **MUCH** better (TCP/IP)

© SPEA. Used with permission

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 2: Enable private conversations between any two parties even if they have not communicated before**
  - Diffie-Hellman-Lamport achieved this (1976) using SKD techniques
    - But it required low cost key distribution channels for *m* keys
    - PKD was selected (partly) due to SKD enrolment cost/scalability
  - **TODAY:** Old barriers no longer apply
    - Networks are **MUCH** better (TCP/IP)
    - 8-bit CPU smart cards are low cost

© SPEA. Used with permission

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 2: Enable private conversations between any two parties even if they have not communicated before**
  - Diffie-Hellman-Lamport achieved this (1976) using SKD techniques
    - But it required low cost key distribution channels for *m* keys
    - PKD was selected (partly) due to SKD enrolment cost/scalability
  - **TODAY:** Old barriers no longer apply
    - Networks are **MUCH** better (TCP/IP)
    - 8-bit CPU smart cards are low cost
    - Cost effective smart card enrolment technologies exist

© SPEA. Used with permission

Re-evaluating the original drivers for PKC (Diffie et al)

Re-evaluating the original drivers for PKC (Diffie et al)

➠ **Driver 3: Enable (mutual) authentication of communicating parties**

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 3: Enable (mutual) authentication of communicating parties**
  - Achievable in 1976 using either PKD or SKD techniques

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 3: Enable (mutual) authentication of communicating parties**
  - Achievable in 1976 using either PKD or SKD techniques
    - SKD methods have the benefits of:
      - All identities discoverable in one location

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 3: Enable (mutual) authentication of communicating parties**
  - Achievable in 1976 using either PKD or SKD techniques
    - SKD methods have the benefits of:
      - All identities discoverable in one location
      - The freshest key material always supplied to users

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 3: Enable (mutual) authentication of communicating parties**
  - Achievable in 1976 using either PKD or SKD techniques
    - SKD methods have the benefits of:
      - All identities discoverable in one location
      - The freshest key always supplied to users

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 3: Enable (mutual) authentication of communicating parties**
  - Achievable in 1976 using either PKD or SKD techniques
    - SKD methods have the benefits of:
      - All identities discoverable in one location
      - The freshest key always supplied to users
  - PKC/PKI systems require digital signatures/certificates

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 3: Enable (mutual) authentication of communicating parties**
  - Achievable in 1976 using either PKD or SKD techniques
    - SKD methods have the benefits of:
      - All identities discoverable in one location
      - The freshest key always supplied to users
  - PKC/PKI systems require digital signatures/certificates
    - Unfortunately, PKI transferred the burden of public key life-cycle management (the discovery and validation of certificates) away from the server ⇒ and towards ⇒ the end user

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 3: Enable (mutual) authentication of communicating parties**
  - Achievable in 1976 using either PKD or SKD techniques
    - SKD methods have the benefits of:
      - All identities discoverable in one location
      - The freshest key always supplied to users
  - PKC/PKI systems require digital signatures/certificates
    - Unfortunately, PKI transferred the burden of public key life-cycle management (the discovery and validation of certificates) away from the server ⇒ and towards ⇒ the end user
    - Many argue today that this key-management burden prevents the ubiquitous take up of encryption (NITRD, Voltage, ...)

Re-evaluating the original drivers for PKC (Diffie et al)

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 4: Remove the need for online servers (Big Driver in 1976)**

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 4: Remove the need for online servers (Big Driver in 1976)**
  - TODAY this requirement is inverted:
    - PKI needs ONLINE servers for SCALABLE revocation systems

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 4: Remove the need for online servers (Big Driver in 1976)**
  - TODAY this requirement is inverted:
    - PKI needs ONLINE servers for SCALABLE revocation systems
    - PKI "Online Certificate Status Protocol" requires digital signatures because there are no prior shared secrets

Re-evaluating the original drivers for PKC (Diffie et al)

- **Driver 4: Remove the need for online servers (Big Driver in 1976)**
  - TODAY this requirement is inverted:
    - PKI needs ONLINE servers for SCALABLE revocation systems
    - PKI "Online Certificate Status Protocol" requires digital signatures because there are no prior shared secrets

PKI is expensive to scale online due to the CPU overhead in signing for OCSP

Re-evaluating the original drivers for PKC (Diffie et al)

Re-evaluating the original drivers for PKC (Diffie et al)

- Today, PKI is used in literally billions of devices
    - Mainstream public key crypto is known to catastrophically fail after the arrival of large code-breaking quantum computers

Re-evaluating the original drivers for PKC (Diffie et al)

- Today, PKI is used in literally billions of devices
  - Mainstream public key crypto is known to catastrophically fail after the arrival of large code-breaking quantum computers
  - Symmetric crypto techniques can accommodate quantum computers and remain secure in practice

Re-evaluating the original drivers for PKC (Diffie et al)

- Today, PKI is used in literally billions of devices
    - Mainstream public key crypto is known to catastrophically fail after the arrival of large code-breaking quantum computers
    - Symmetric crypto techniques can accommodate quantum computers and remain secure in practice
    - NIST CKM Workshop identified that CKM designers should look towards new solutions that are post quantum secure and that do not rely on PKC (that is, use symmetric techniques)

Re-evaluating the original drivers for PKC (Diffie et al)

- Today, PKI is used in literally billions of devices
  - Mainstream public key crypto is known to catastrophically fail after the arrival of large code-breaking quantum computers
  - Symmetric crypto techniques can accommodate quantum computers and remain secure in practice
  - NIST CKM Workshop identified that CKM designers should look towards new solutions that are post quantum secure and that do not rely on PKC (that is, use symmetric techniques)
  - Symmetric cryptosystems are complementary to public key cryptosystems and can be combined together.

Re-evaluating the original drivers for PKC (Diffie et al)

Re-evaluating the original drivers for PKC (Diffie et al)

- Today:
  - There have been Radical changes in the technology landscape since 1976

Re-evaluating the original drivers for PKC (Diffie et al)

- Today:
  - There have been Radical changes in the technology landscape since 1976
  - Online remotely managed services (hosted in the Cloud) are becoming increasingly attractive

Re-evaluating the original drivers for PKC (Diffie et al)

- Today:
  - There have been Radical changes in the technology landscape since 1976
  - Online remotely managed services (hosted in the Cloud) are becoming increasingly attractive
  - Online Symmetric IdM/CKM architectures make more sense then they did in 1970-1980's

Evolving the democratic principles of 'Spirit of Laws' into security systems

Charles de Secondant,
Public domain image

Evolving the democratic principles of ‘Spirit of Laws’ into security systems

- ‘Spirit of Laws’ is a treatise on political theory (1748)
- *Objective: Reduce citizens fear of the political system*

Charles de Secondant, Public domain image

Evolving the democratic principles of 'Spirit of Laws' into security systems

- 'Spirit of Laws' is a treatise on political theory (1748)
- *Objective: Reduce citizens fear of the political system*
- It advocated:
  - constitutionalism
  - separation of powers
  - a system of checks & balances
  - preservation of civil liberties

Charles de Secondant,
Public domain image

Evolving the democratic principles of ‘Spirit of Laws’ into security systems

Charles de Secondant,
Public domain image

Evolving the democratic principles of ‘Spirit of Laws’ into security systems

Charles de Secondant,
Public domain image

- These principles underpin democratic Governments
- Enabling citizens to have some confidence/trust in the integrity of the political system

Evolving the democratic principles of ‘Spirit of Laws’ into security systems

Charles de Secondant, Public domain image

- These principles underpin democratic Governments
- Enabling citizens to have some confidence/trust in the integrity of the political system
- TODAY:
  - we can be embodied these principles into cybersecurity systems
  - to protect the legitimate and diversified interests of all stakeholders, even in a global context

Evolving the democratic principles of ‘Spirit of Laws’ into security systems

Charles de Secondant,
Public domain image

- These principles underpin democratic Governments
- Enabling citizens to have some confidence/trust in the integrity of the political system
- TODAY:

Evolving the democratic principles of 'Spirit of Laws' into security systems

Charles de Secondant, Public domain image

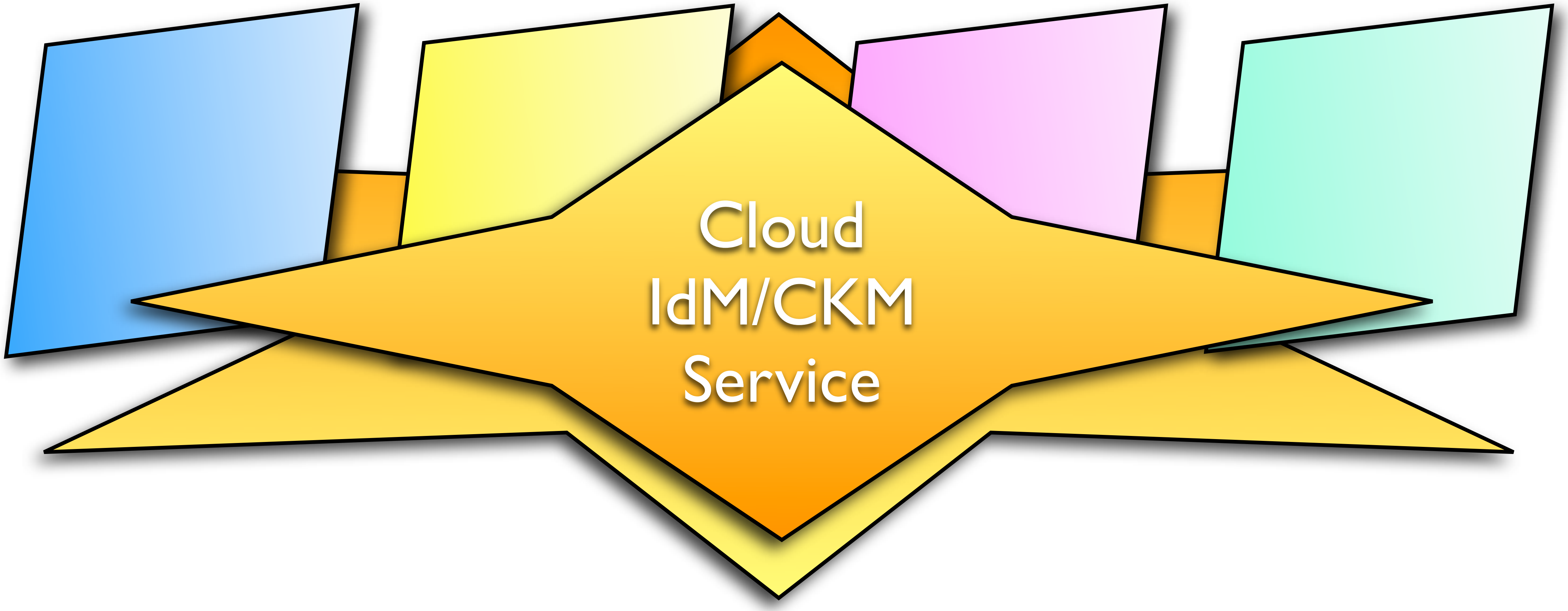
- These principles underpin democratic Governments
- Enabling citizens to have some confidence/trust in the integrity of the political system
- TODAY:
  - Cyber security can support democratic institutions

Evolving the democratic principles of ‘Spirit of Laws’ into security systems

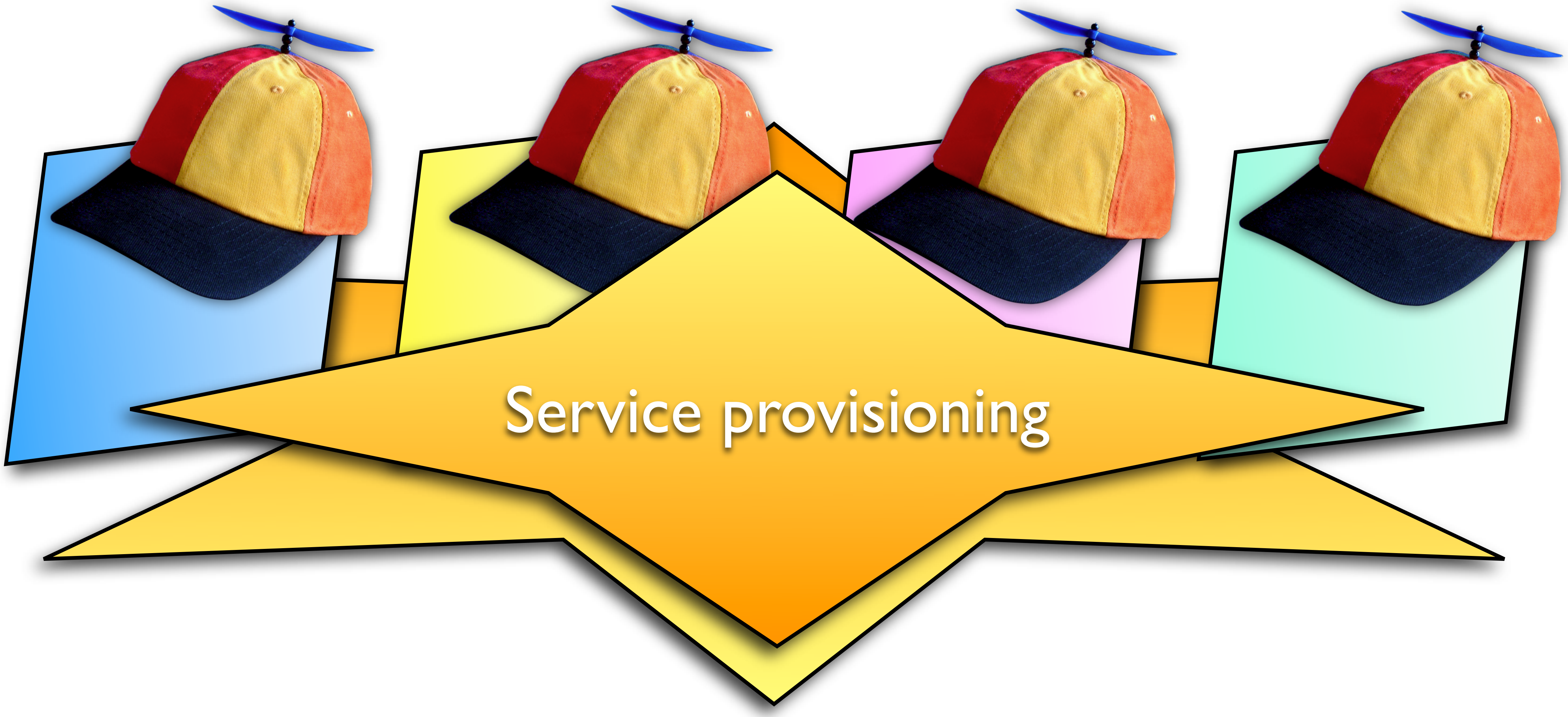
Charles de Secondant, Public domain image

- These principles underpin democratic Governments
- Enabling citizens to have some confidence/trust in the integrity of the political system
- TODAY:
  - Cyber security can support democratic institutions
  - We can limit potential for unilateral global attacks by authoritarian regimes and individuals (*Unlike PKI where it is possible today for any one PKI Root Certificate Authority to subvert Identity Assertions against any user/organisation, located in any country, in any civilian namespace, on the civilian Internet*)

High level overview of Synaptic's proposed IdM/CKM architecture from 10'000 ft

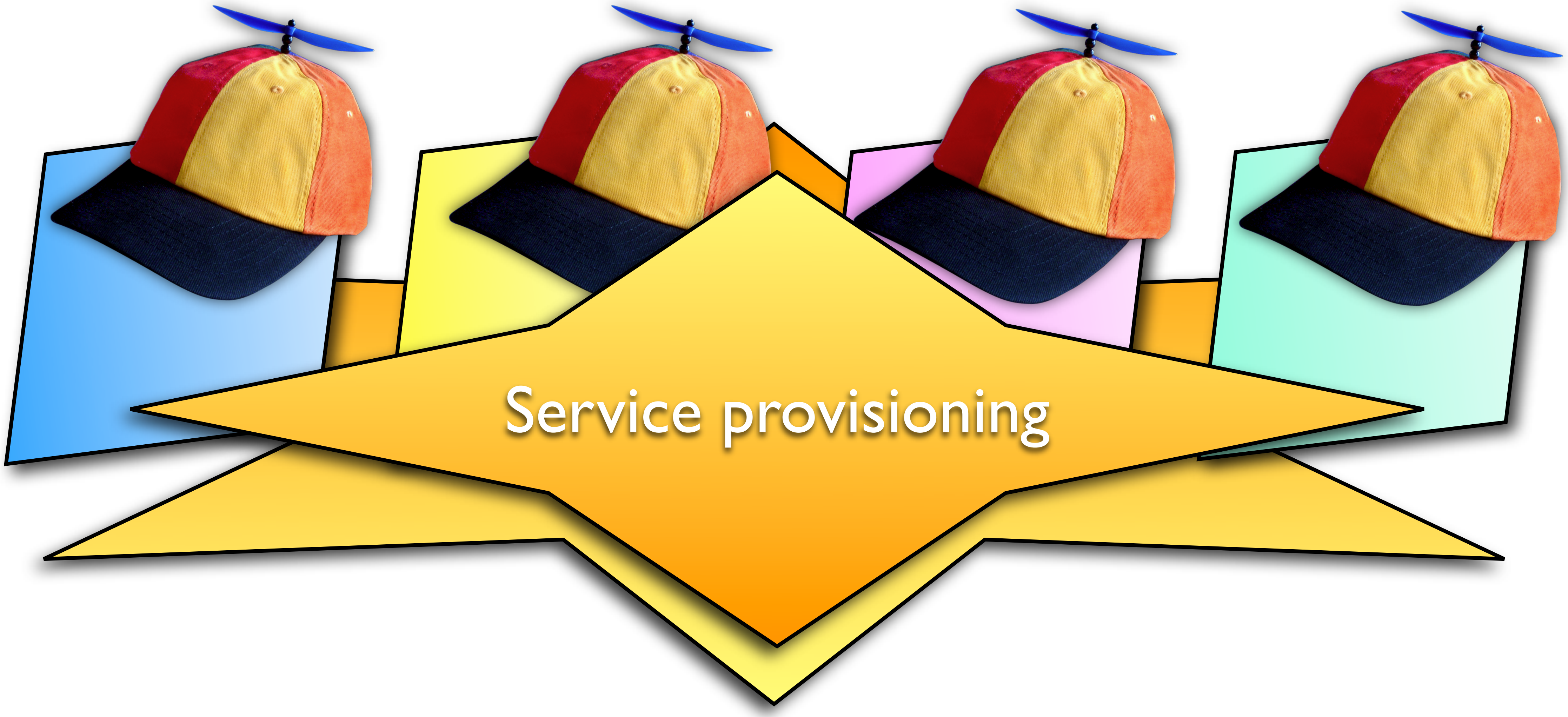


10,000 ft: Distribute trust over *m* providers



Beanies: © Geek Culture, used with permission.

10,000 ft: Distribute trust over *m* providers



➠ **Provision each transaction across *m* independent service providers to distribute trust and remove single points of failure**

Beanies: © Geek Culture, used with permission.

10,000 ft: (m-1) Collusion resistance

- Provision each transaction across *m* independent service providers to distribute trust and remove single points of failure

Beanies: © Geek Culture, used with permission.

10,000 ft: (m-1) Collusion resistance

- Provision each transaction across *m* independent service providers to distribute trust and remove single points of failure
- **To resist a collusion/failure of (*m*-1) out of *m* service providers**

Beanies: © Geek Culture, used with permission.

10,000 ft: Protection against insider attacks

- Mitigating <u>insider attacks</u> is a focus area for the U.S. Oak Ridge National Laboratory and various other US cyber security initiatives

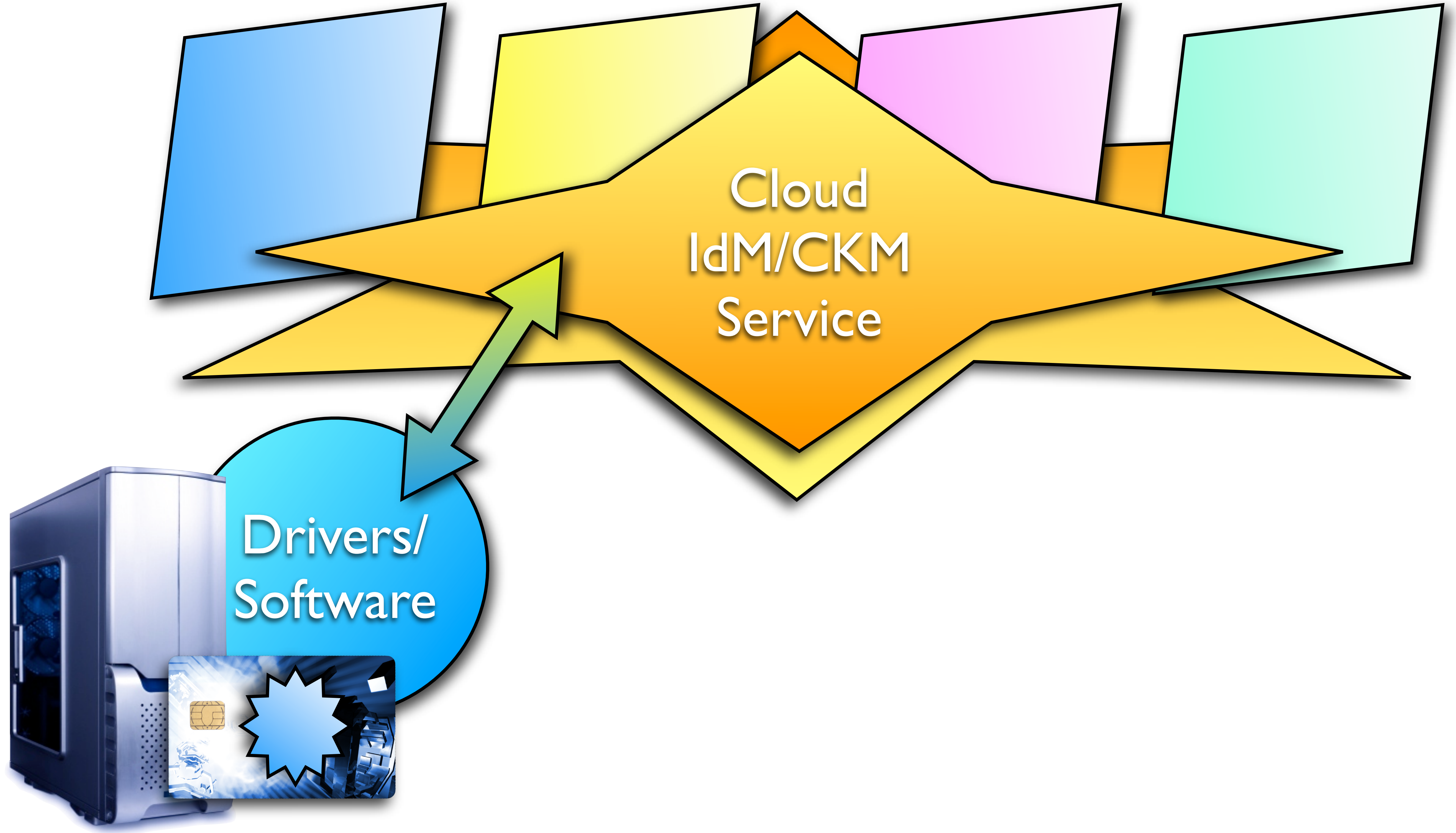
Beanies: © Geek Culture, used with permission.

10,000 ft: Protection against insider attacks

- Mitigating insider attacks is a focus area for the U.S. Oak Ridge National Laboratory and various other US cyber security initiatives
- We can use untrusted outsiders to hedge against trusted insiders...

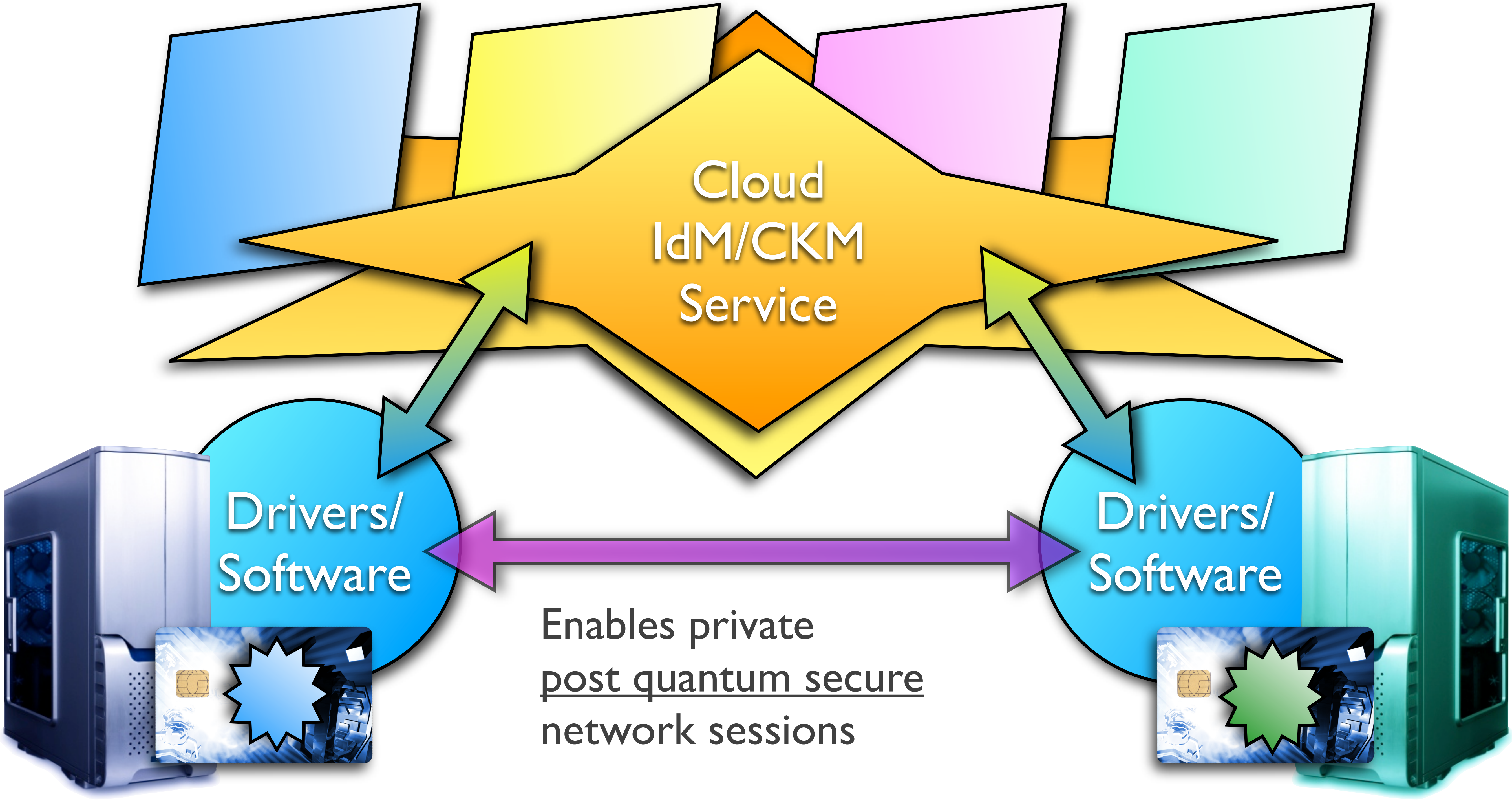
Beanies: © Geek Culture, used with permission.

10,000 ft: Providers, Software, Tokens, Desktops...



Computers © iStockPhoto, Background on smart card © Inmagine, Used with permission.

10,000 ft: Providers, Software, Tokens, Desktops...

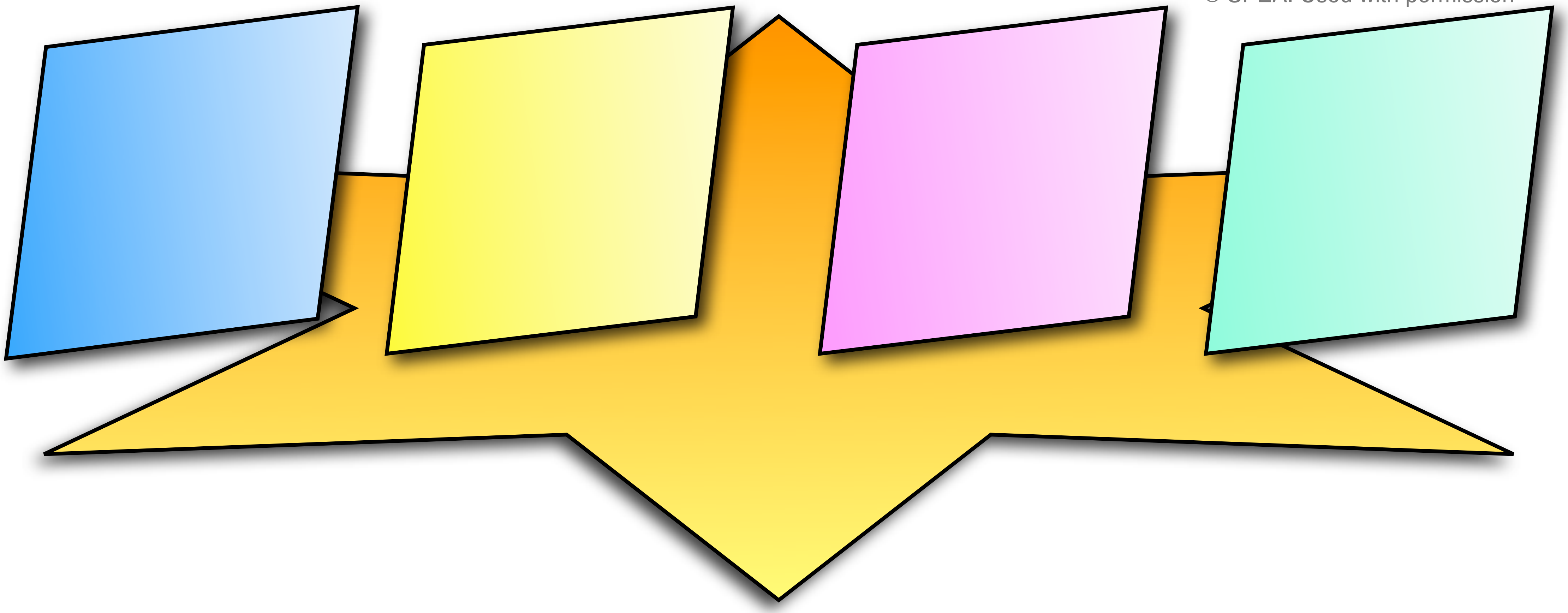


Enables private
post quantum secure
network sessions

Computers © iStockPhoto, Background on smart card © Inmagine, Used with permission.

10,000 ft: Enrolling tokens and their first use

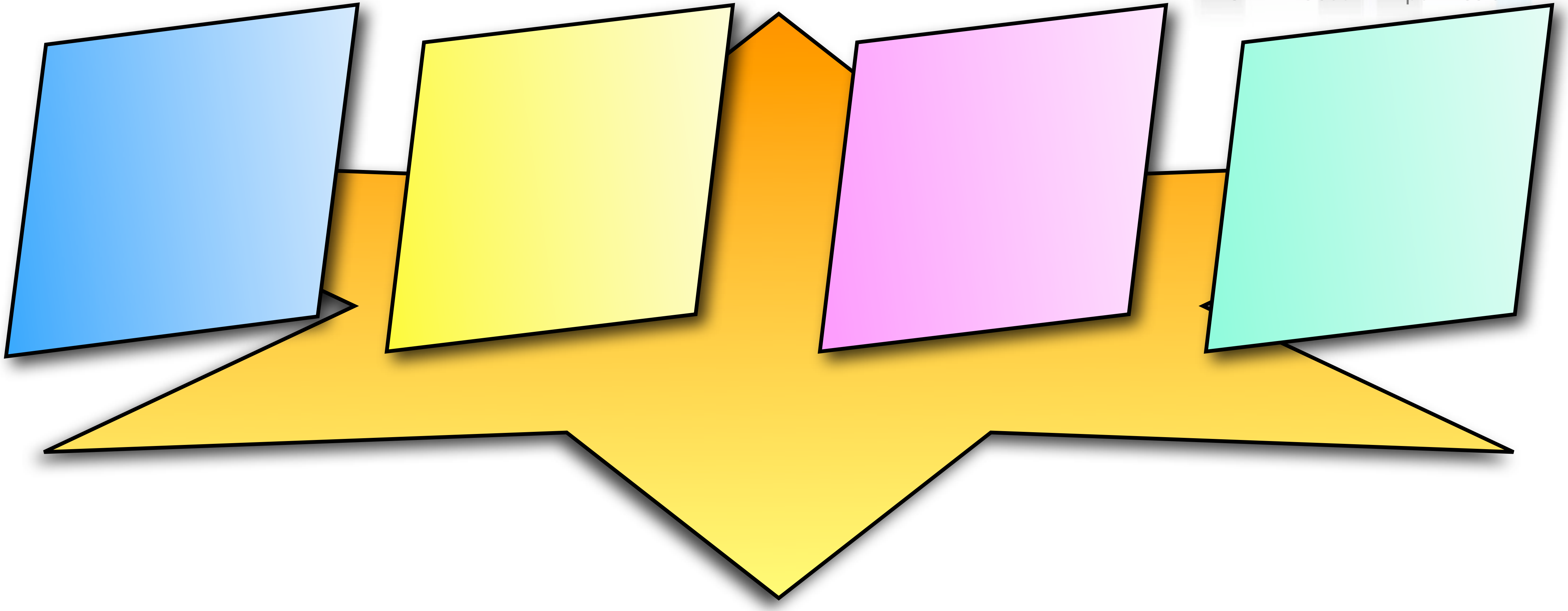
© SPEA. Used with permission



10,000 ft: Enrolling tokens and their first use

- Enrol each token by injecting **m** keys

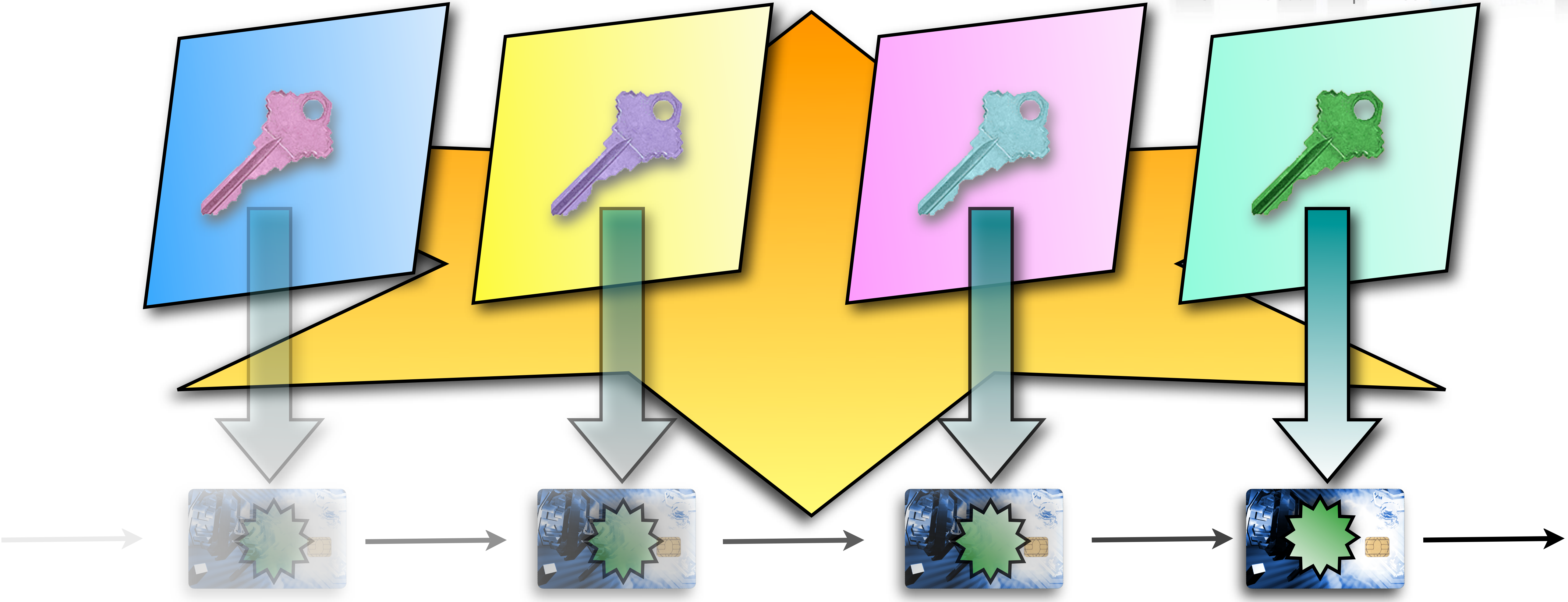
© SPEA. Used with permission



10,000 ft: Enrolling tokens and their first use

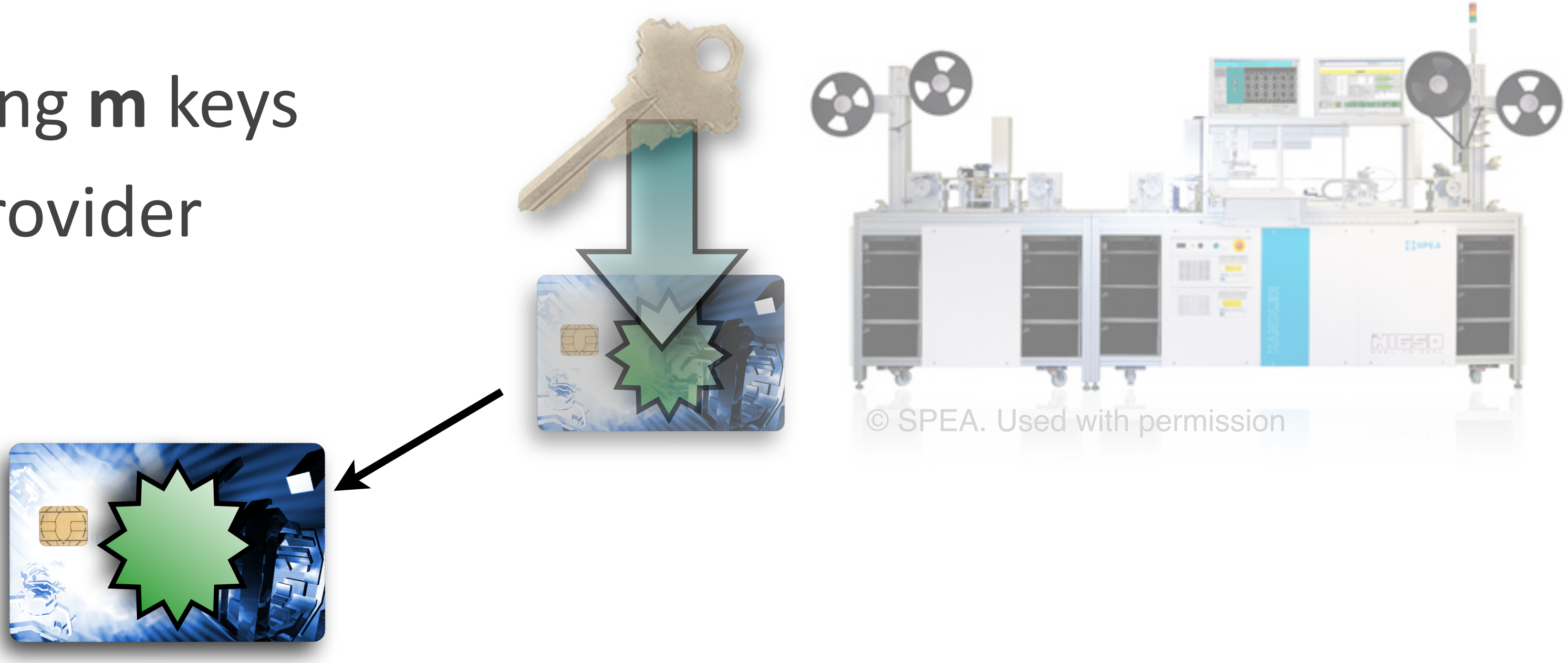
- Enrol each token by injecting **m** keys
  - One key per service provider

© SPEA. Used with permission



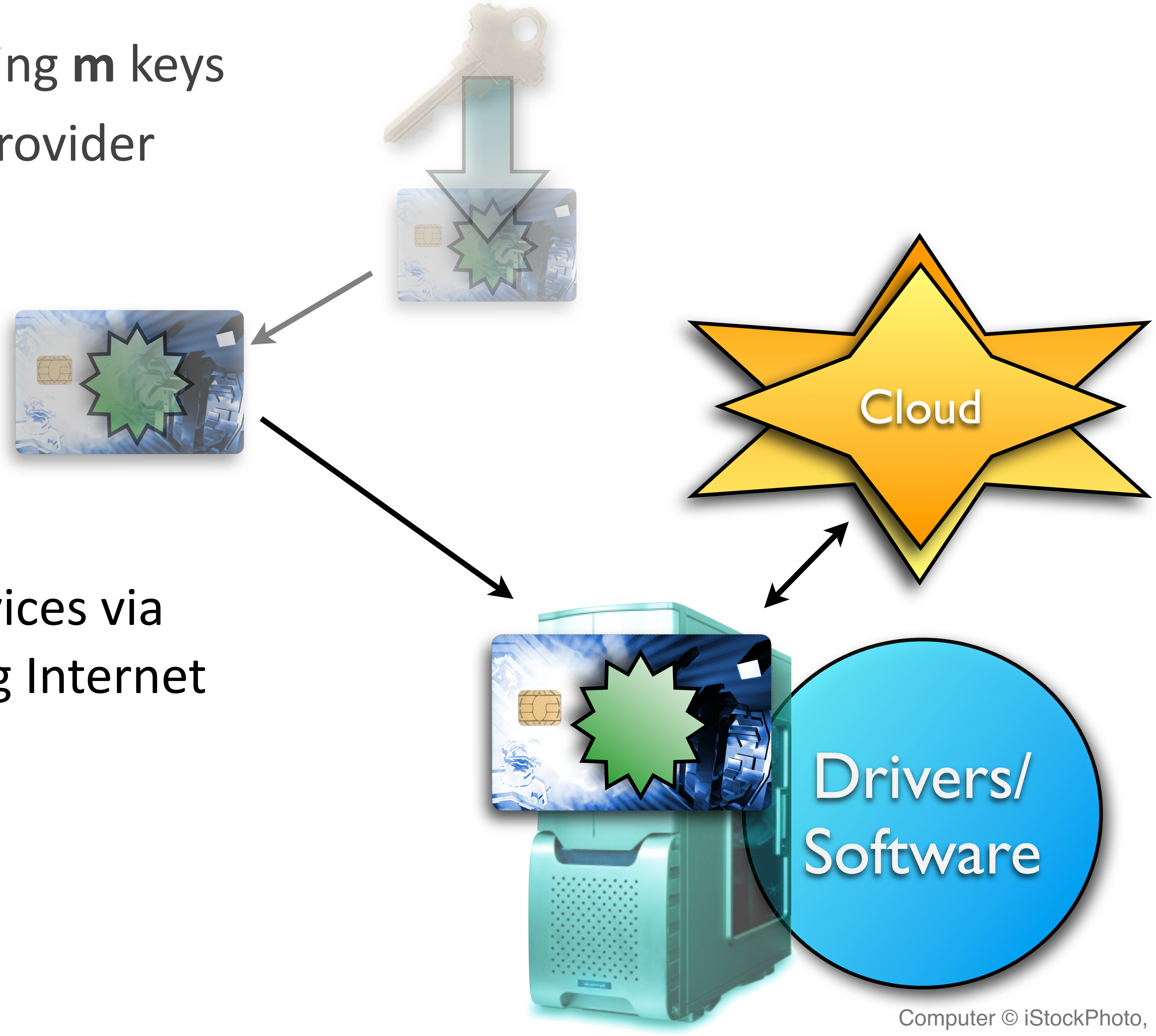
10,000 ft: Enrolling tokens and their first use

- Enrol each token by injecting **m** keys
  - One key per service provider
- Distribute tokens to users


© SPEA. Used with permission

10,000 ft: Enrolling tokens and their first use

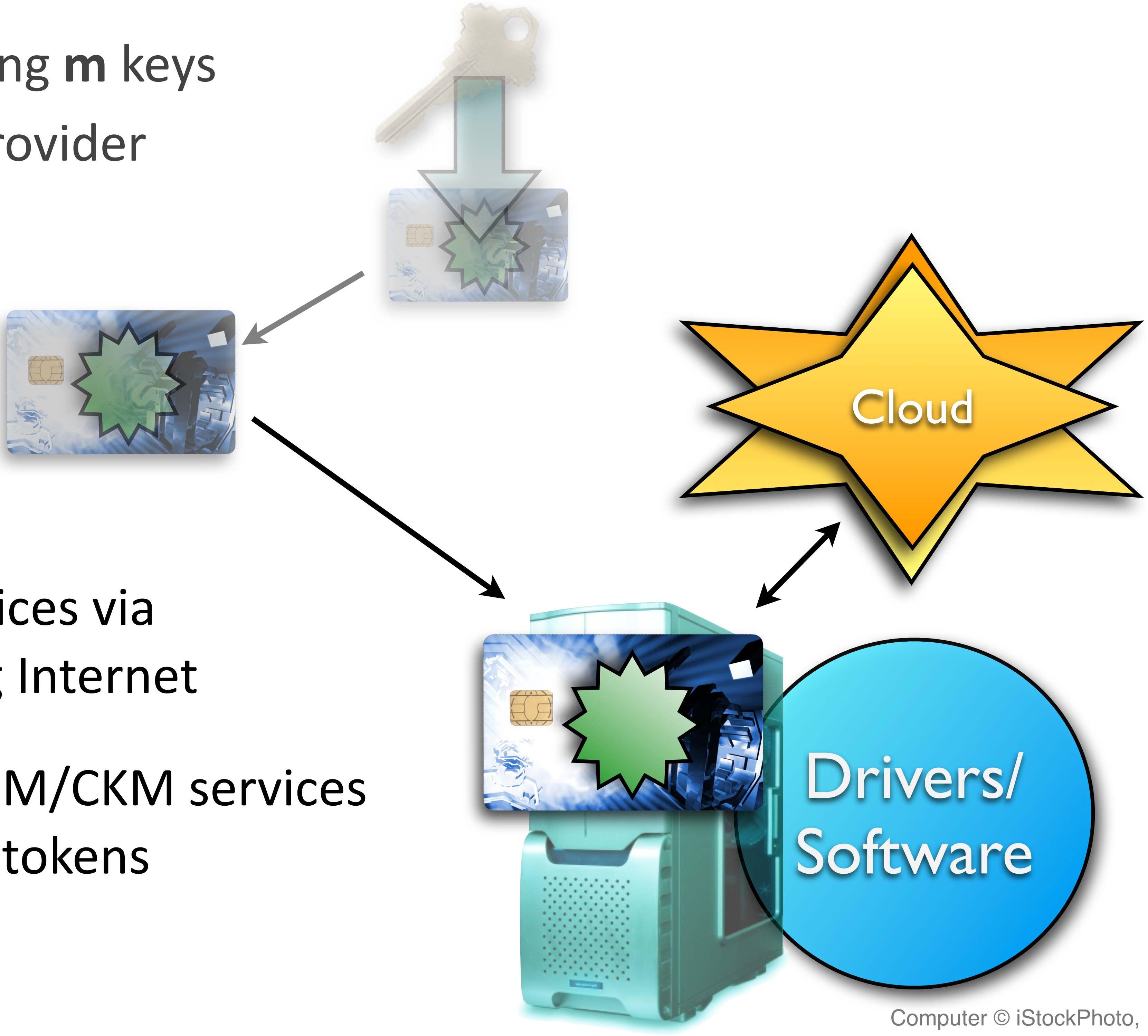
- Enrol each token by injecting **m** keys
  - One key per service provider
- Distribute tokens to users
- Tokens log in to cloud services via software/drivers and using Internet



Computer © iStockPhoto,

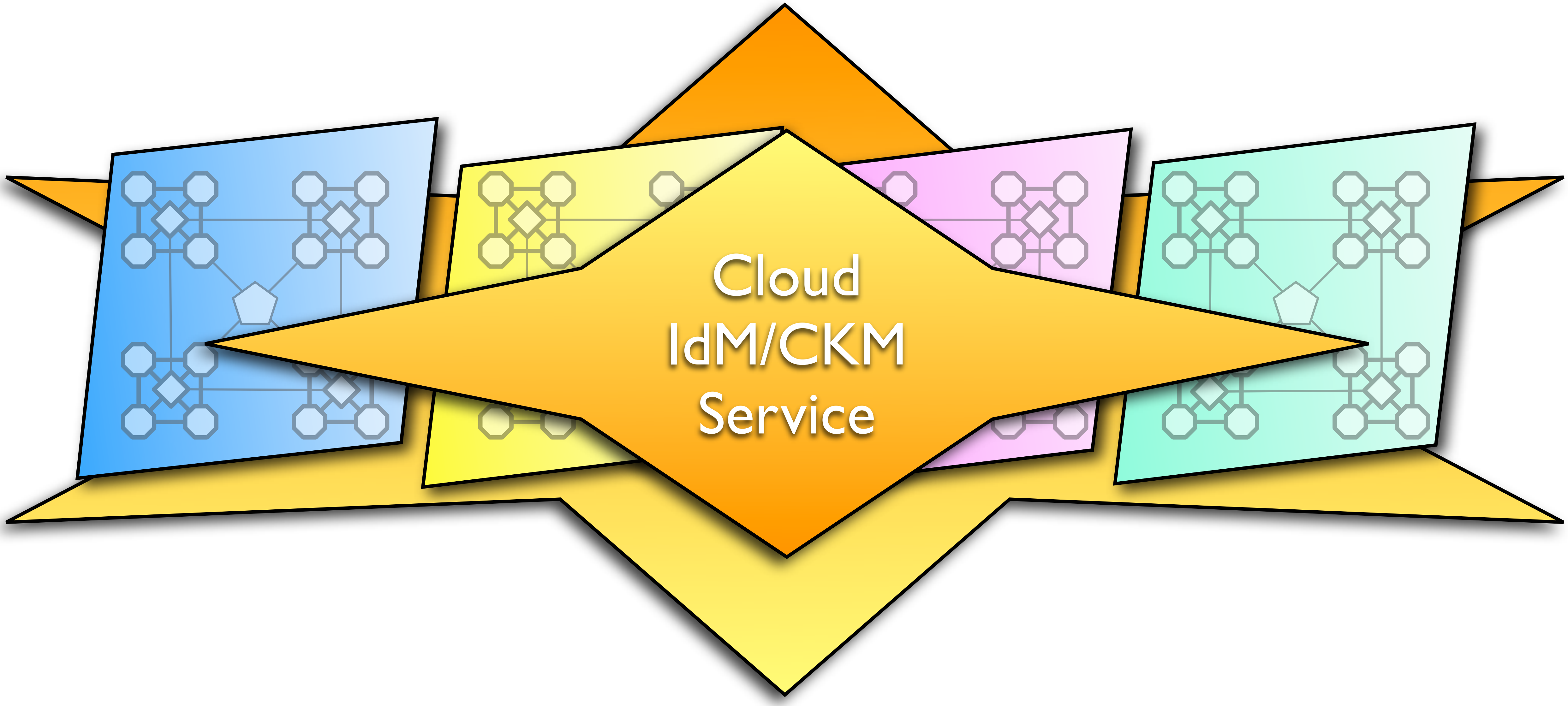
10,000 ft: Enrolling tokens and their first use

- Enrol each token by injecting **m** keys
  - One key per service provider
- Distribute tokens to users
- Tokens log in to cloud services via software/drivers and using Internet
  - Cloud performs <u>first</u> IdM/CKM services on behalf of/between tokens



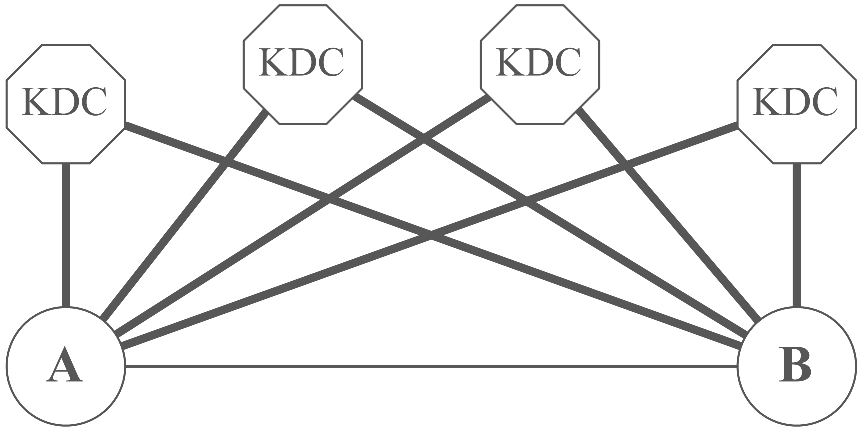
Computer © iStockPhoto,

A short survey of architectural techniques, cryptographic components and applications...

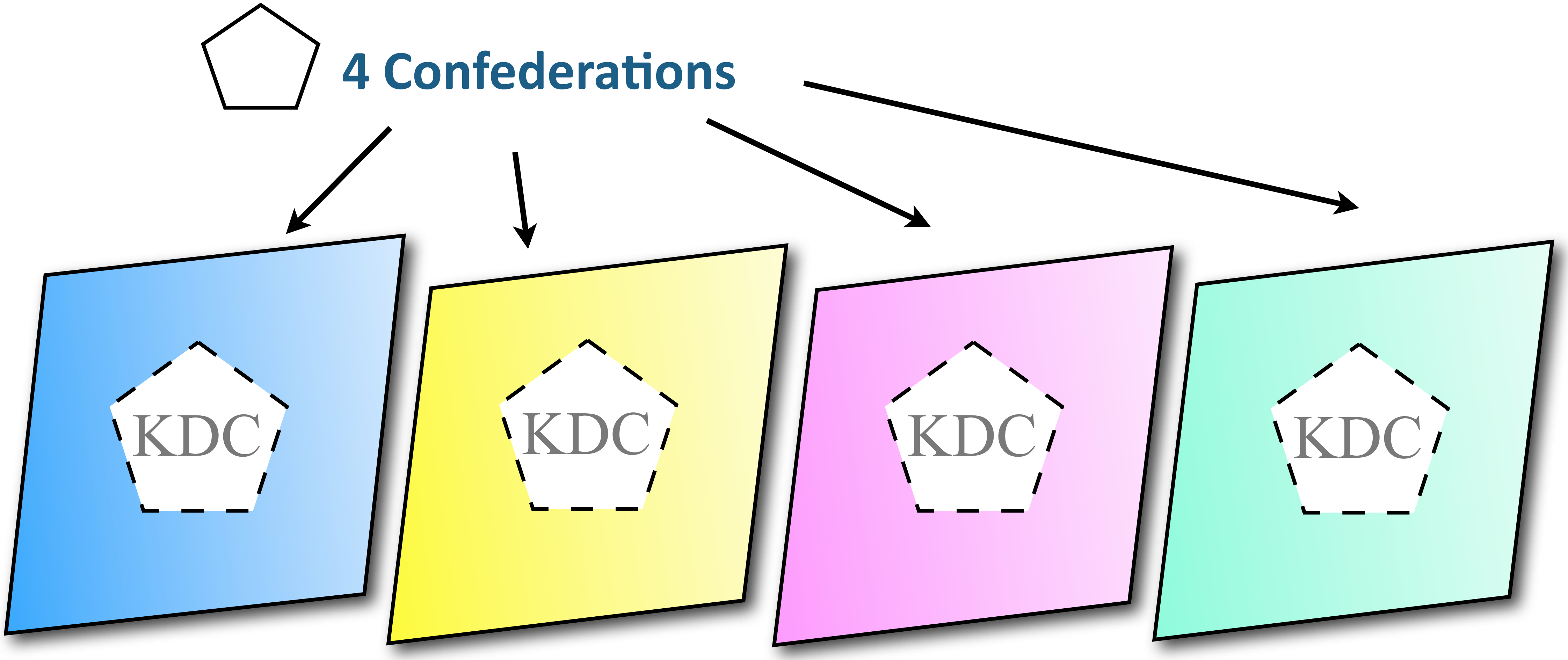


SLL proposal: Topology

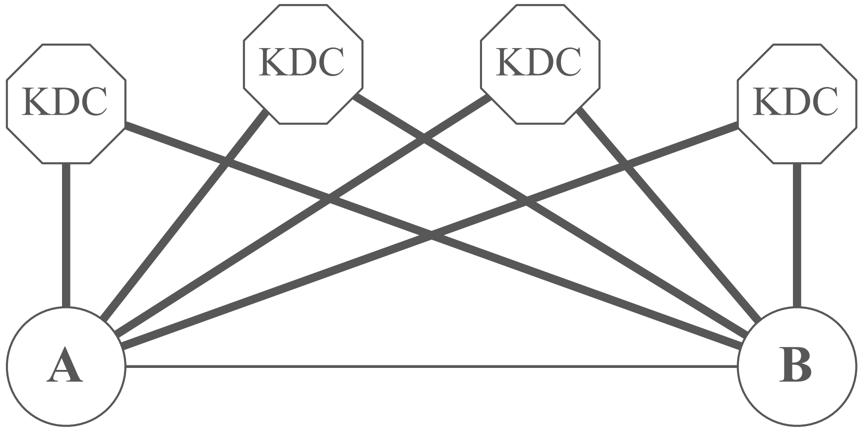
SLL proposal: Topology



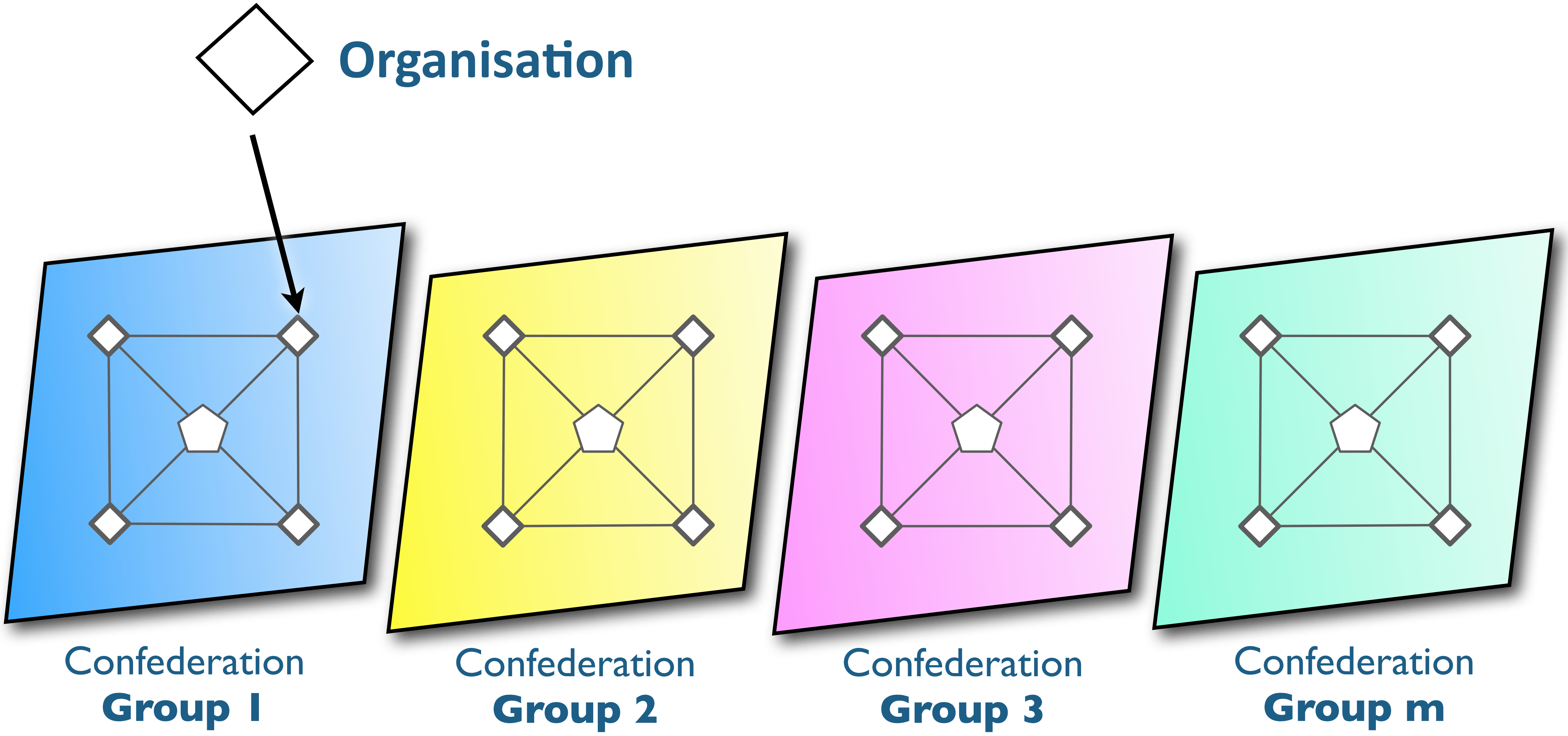
SLL proposal: Topology



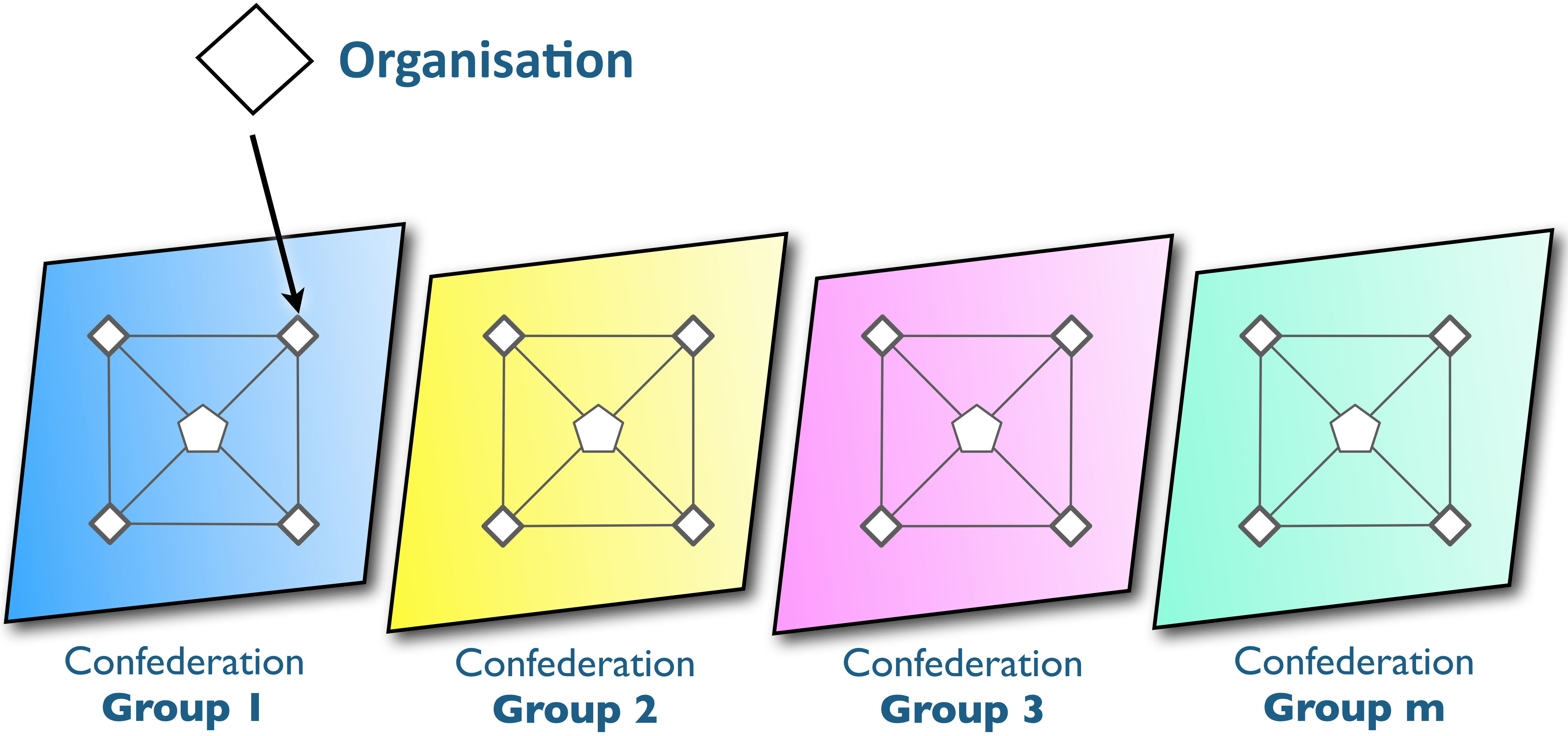
- We substitute the m KDC in the Diffie-Hellman-Lamport 1976 proposal with m confederations



SLL: Abstract confederation topology

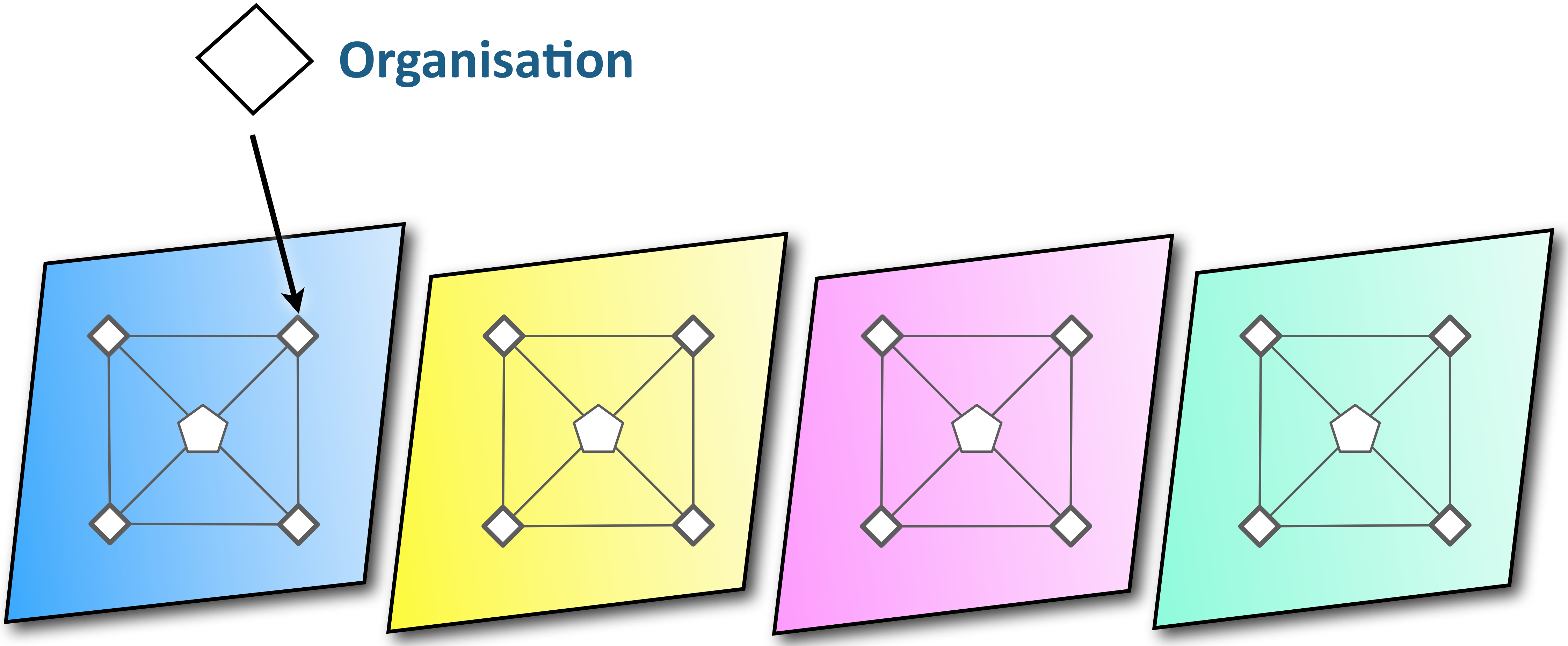


SLL: Abstract confederation topology



- The number of confederations is typically 3 to 7

SLL: Abstract confederation topology



Organisation

Confederation **Group I**

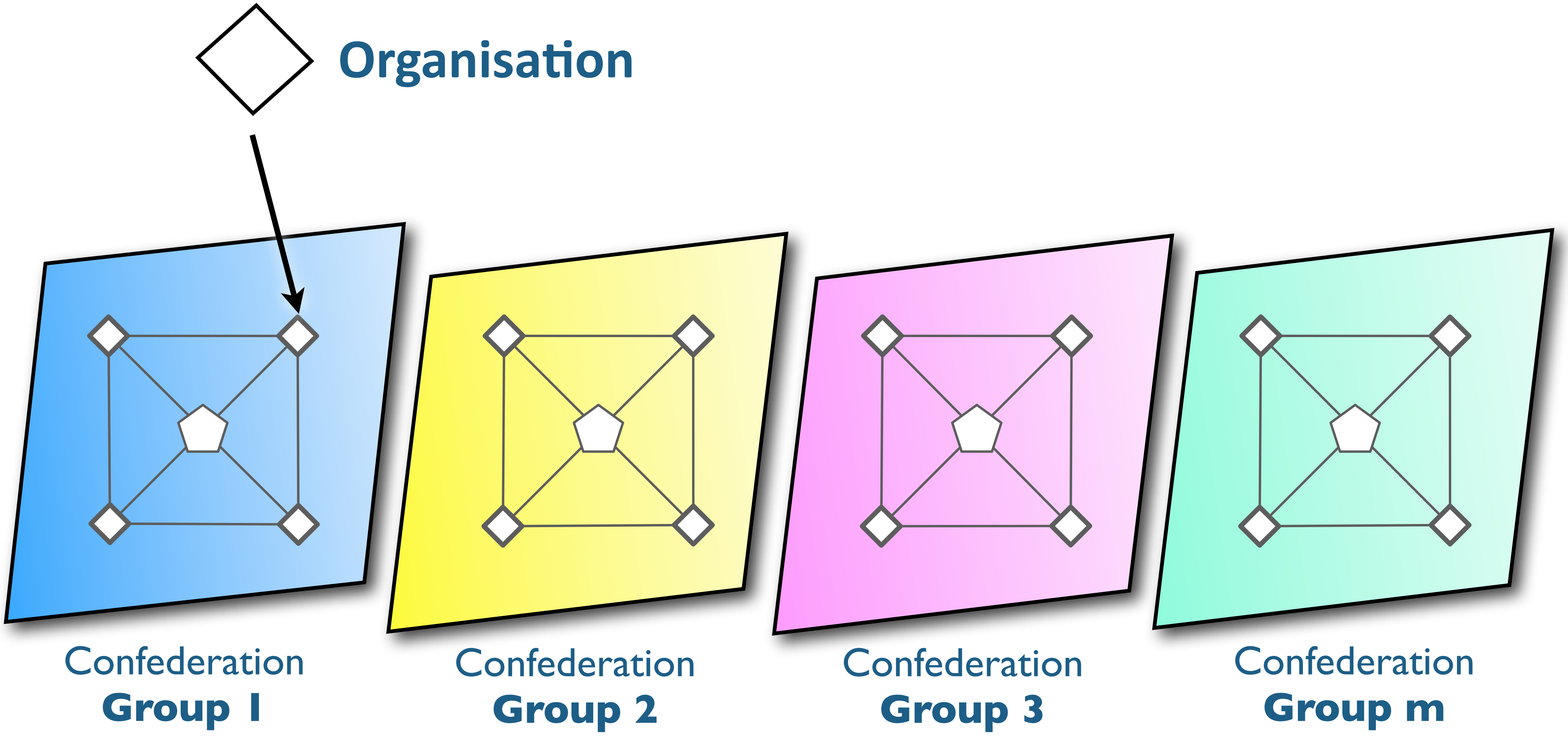
Confederation **Group 2**

Confederation **Group 3**

Confederation **Group m**

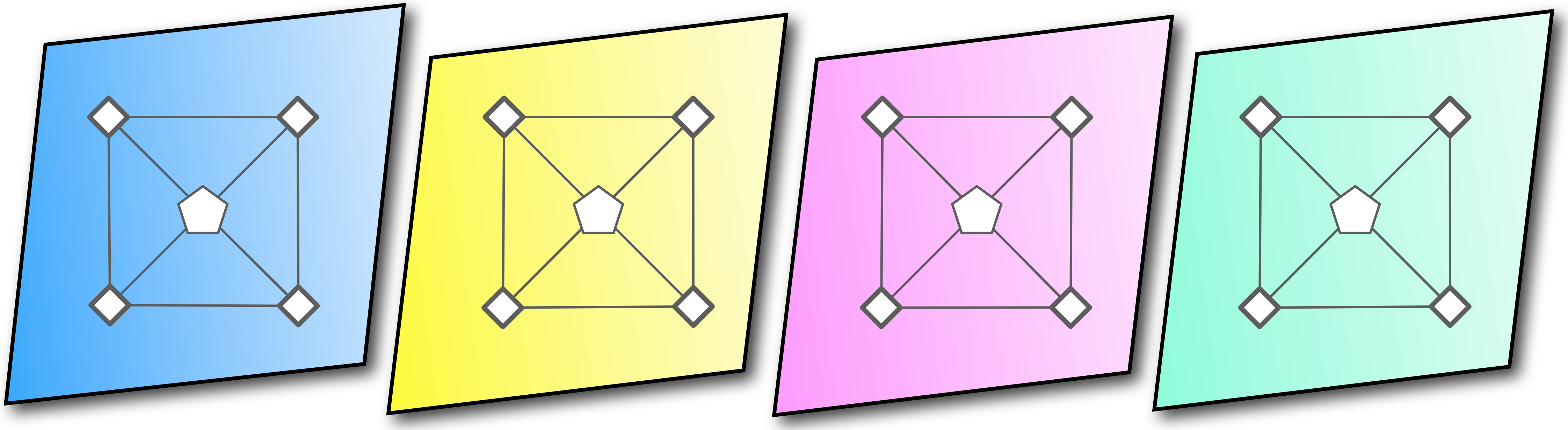
- The number of confederations is typically 3 to 7
- There is typically more than one organisation in each confederation

SLL: Abstract confederation topology

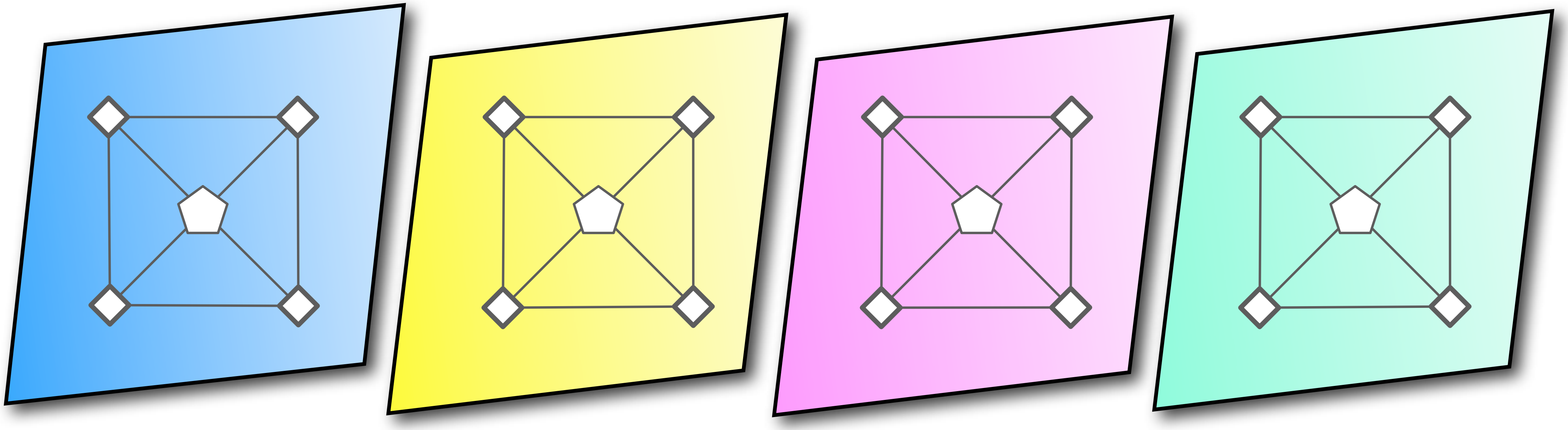


- The number of confederations is typically 3 to 7
- There is typically more than one organisation in each confederation
- Confederations group similar organisations by affiliation or region

SLL: Example Topology - Banks



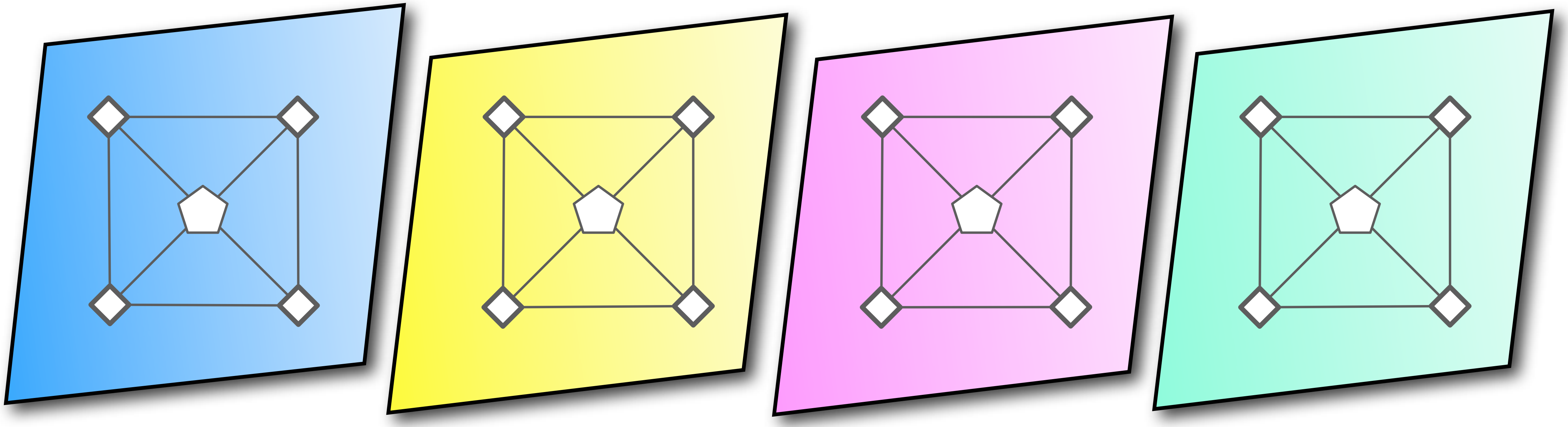
SLL: Example Topology - Banks



➠ It is **desirable** if confederations are traditionally strong competitors

SLL: Example Topology - Banks

WELLS FARGO Bank of America JPMorganChase citibank



Confederation **Wells Fargo**

Confederation **Bank of America**

Confederation **JPMorgan Chase**

Confederation **Citibank**

- It is **desirable** if confederations are traditionally strong competitors
- eg. Each large bank could be represented by a confederation, with each of the offices as a member organisation

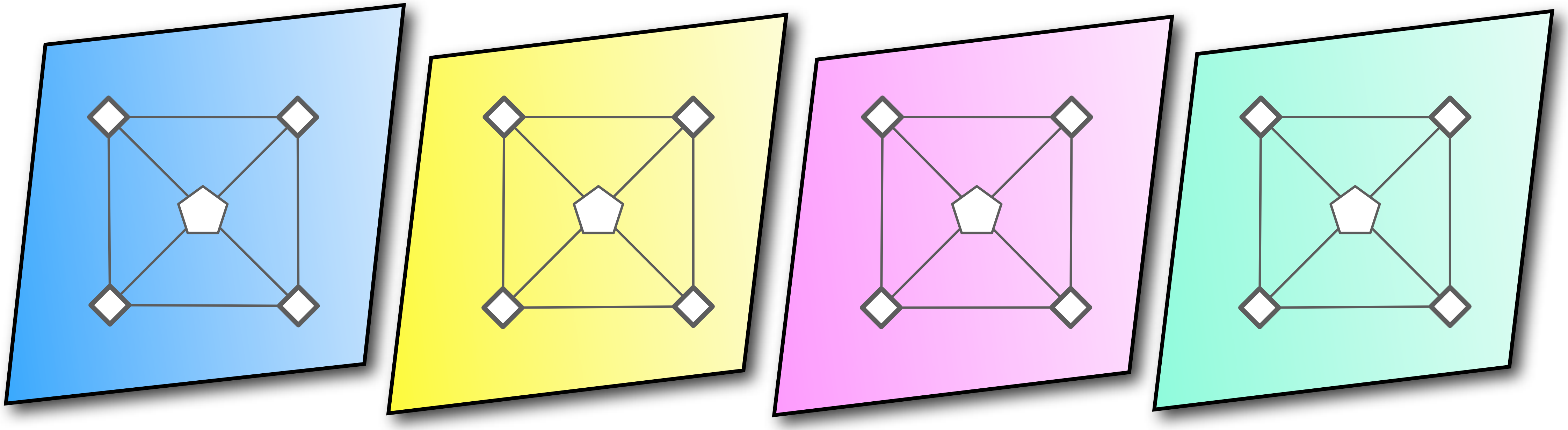
SLL: Example Topology - USA National

Confederation **Finance**

Confederation **Industrial**

Confederation **Retail**

Confederation **Government**



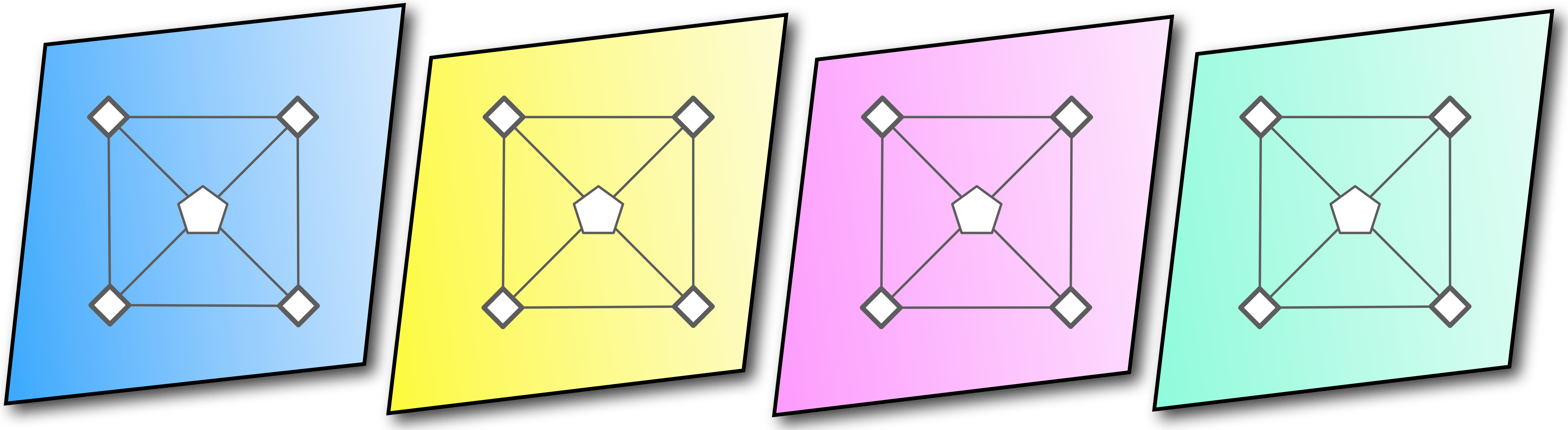
SLL: Example Topology - USA National

Confederation **Finance**

Confederation **Industrial**

Confederation **Retail**

Confederation **Government**



➠ Only one confederation needs to ‘do its job right’ to guarantee security for ALL users of the system, not just users in its own community

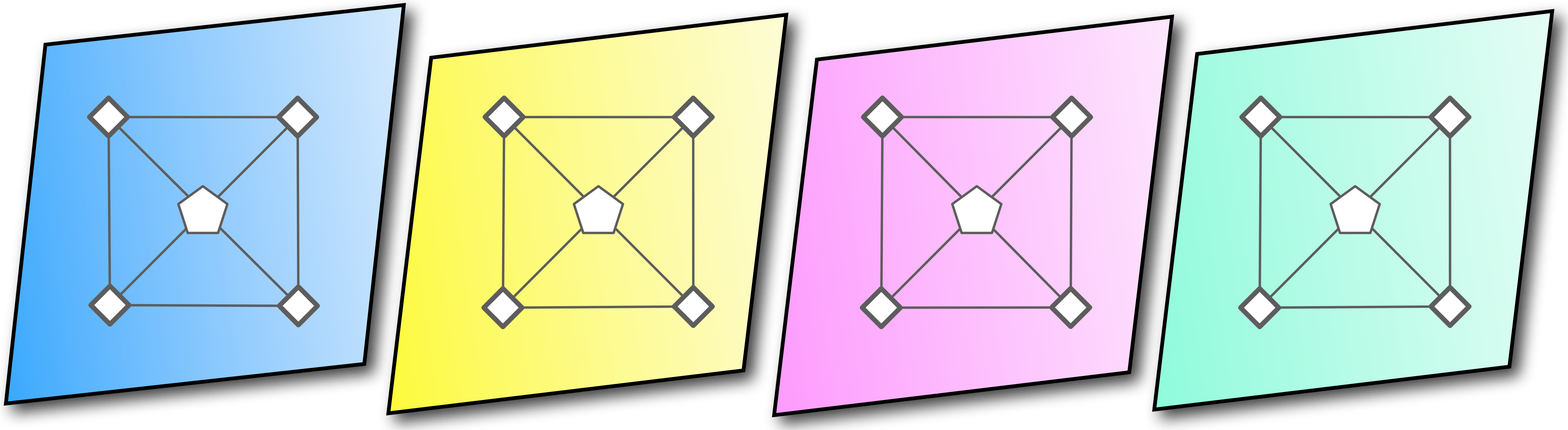
SLL: Example Topology - USA National

Confederation **Finance**

Confederation **Industrial**

Confederation **Retail**

Confederation **Government**



- Only one confederation needs to 'do its job right' to guarantee security for ALL users of the system, not just users in its own community
- **Distributing trust across un-aligned** groups mitigates insider attacks

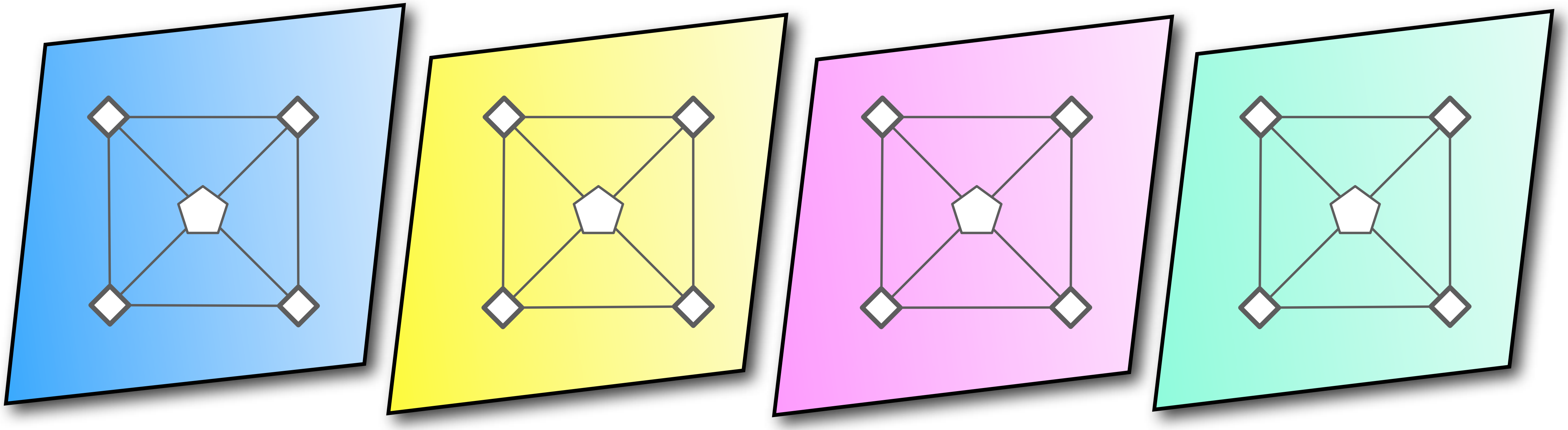
SLL: Example Topology - 5 eyes (aligned countries)

Confederation **USA**

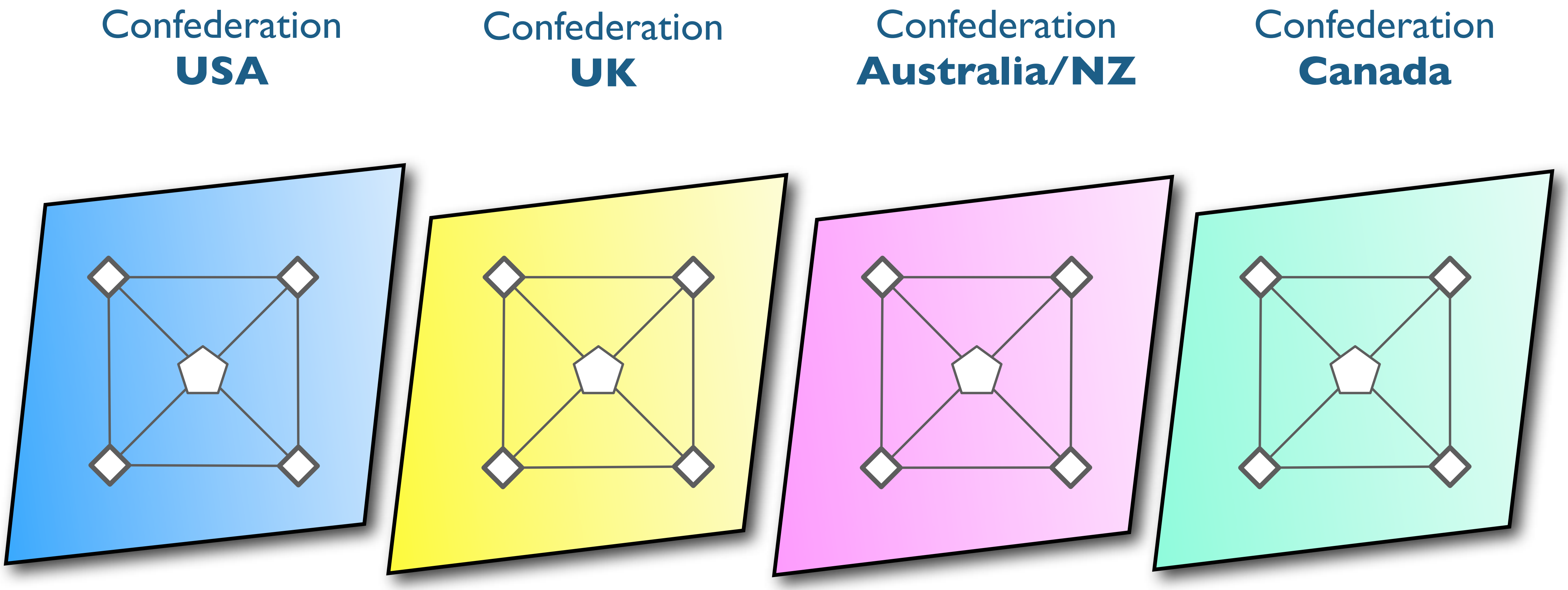
Confederation **UK**

Confederation **Australia/NZ**

Confederation **Canada**



SLL: Example Topology - 5 eyes (aligned countries)



- A system of checks-and-balances can be implemented to ensure correctness of transactions for the stake-holder, and to protect the common interest/good

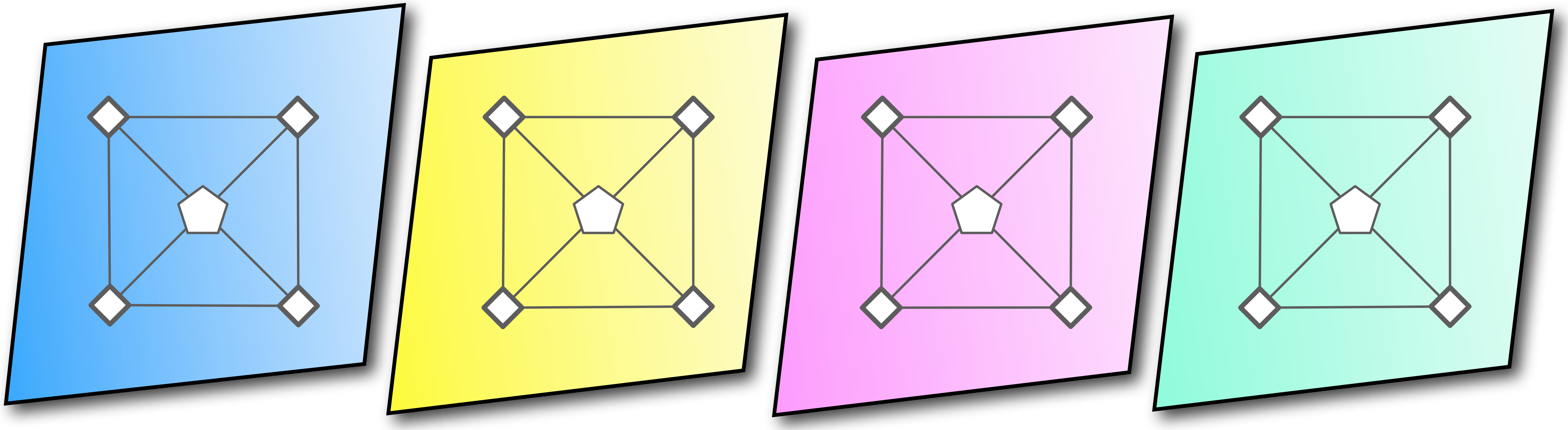
SLL: Example Topology - International

Confederation **Americas**

Confederation **European Union**

Confederation **Asia**

Confederation **Various**



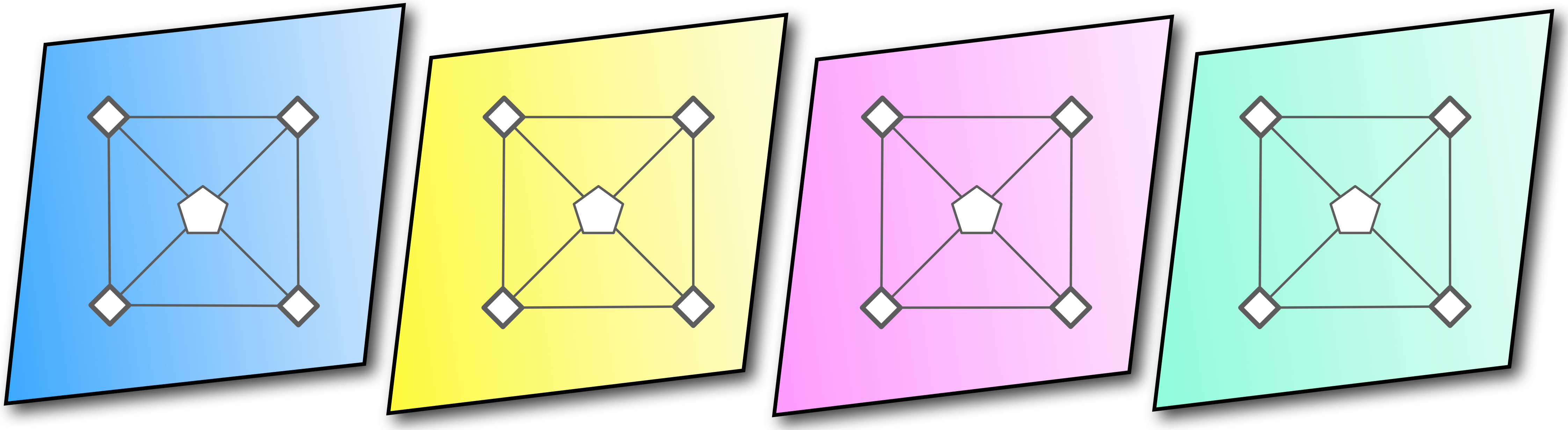
SLL: Example Topology - International

Confederation **Americas**

Confederation **European Union**

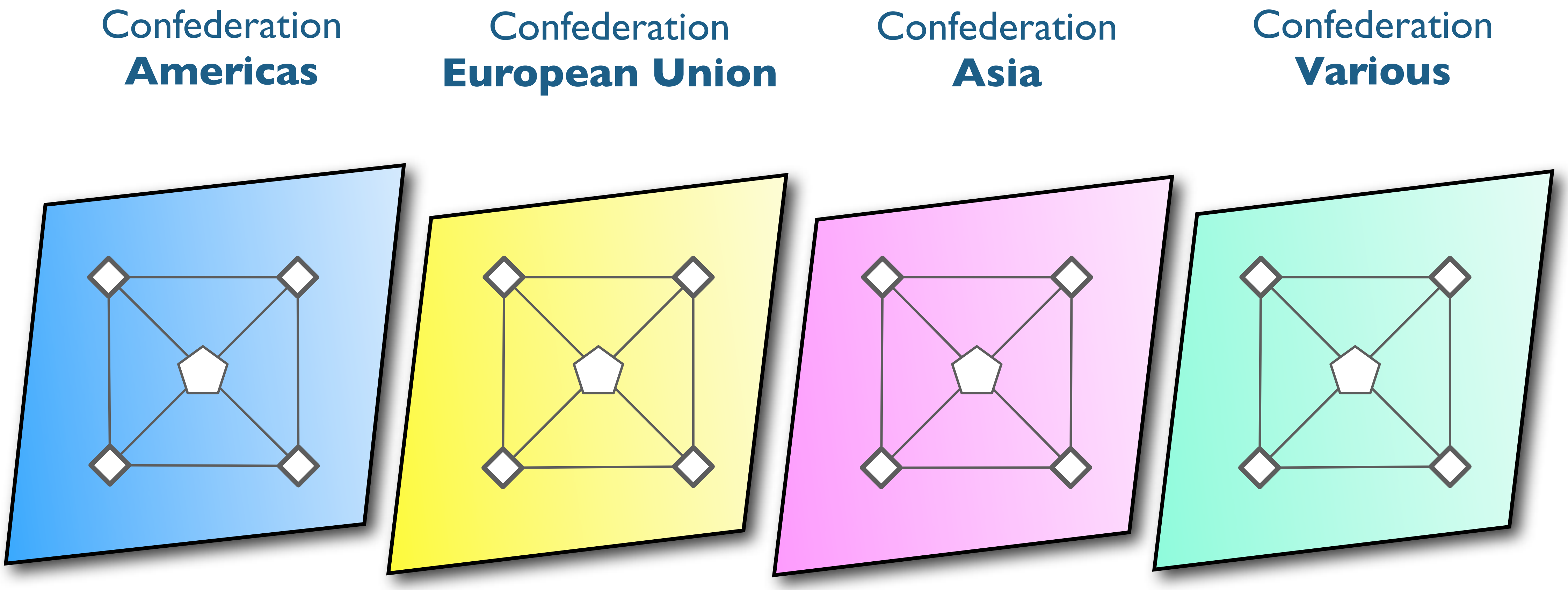
Confederation **Asia**

Confederation **Various**



➠ In an international context, we can group by region

SLL: Example Topology - International



- In an international context, we can group by region
- An international system ensures global inter-connectivity between every token (interoperability)

SLL: A card enrolled in logically different systems

SLL: A card enrolled in logically different systems

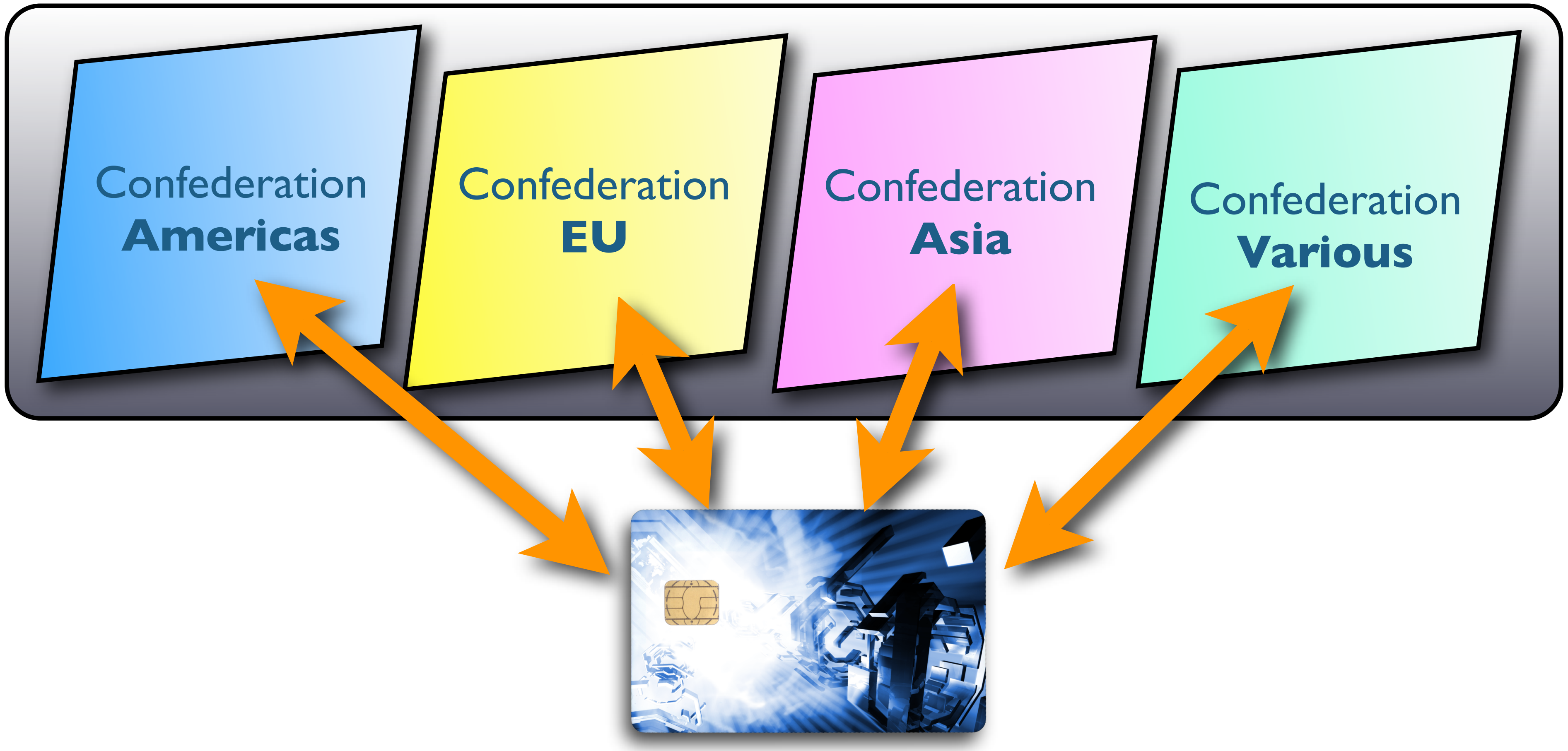
A smart card can be simultaneously enrolled into several logically different systems

SLL: A card enrolled in logically different systems

A smart card can be simultaneously enrolled into several logically different systems

1) International

2) Regional/National



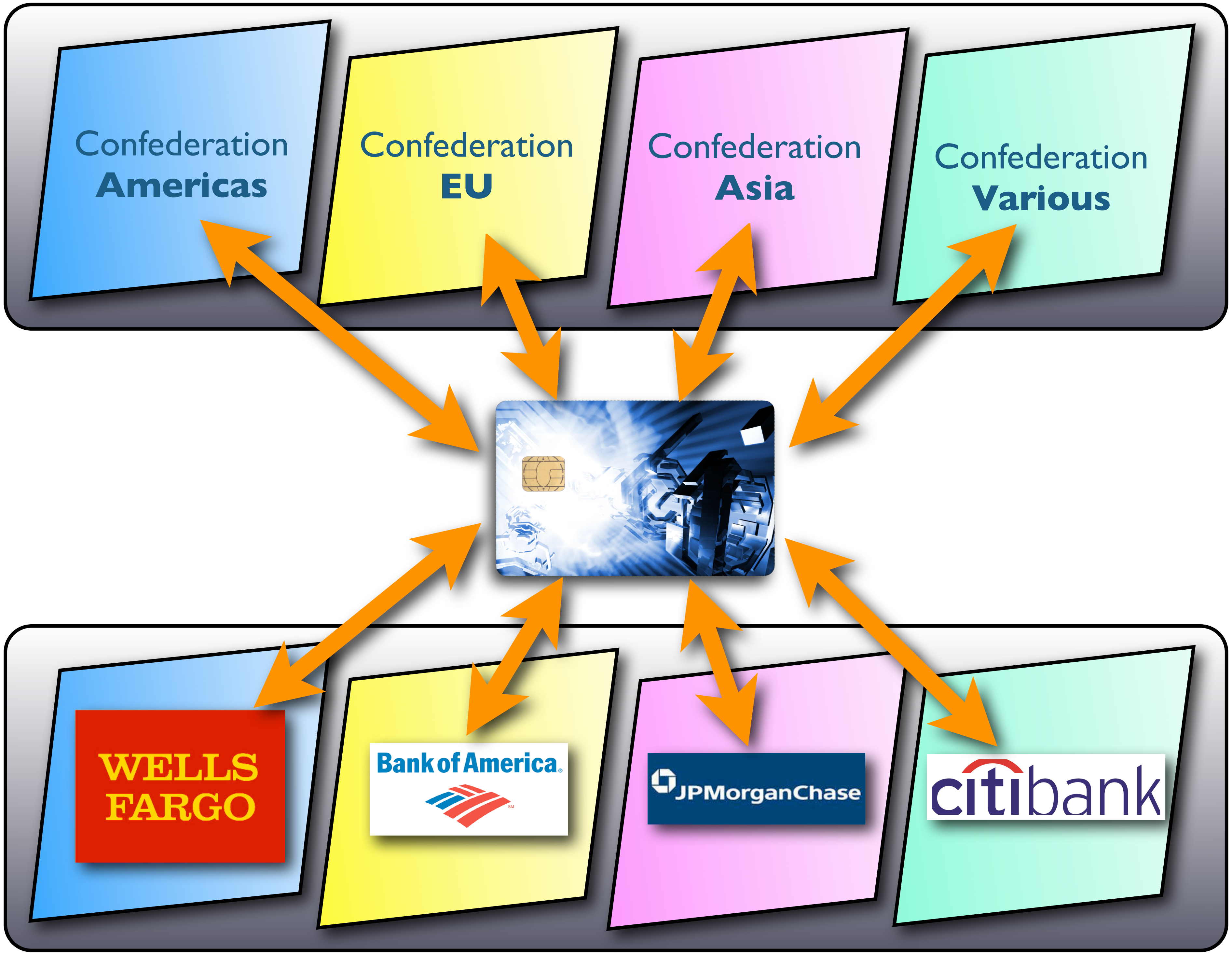
SLL: A card enrolled in logically different systems

A smart card can be simultaneously enrolled into several logically different systems

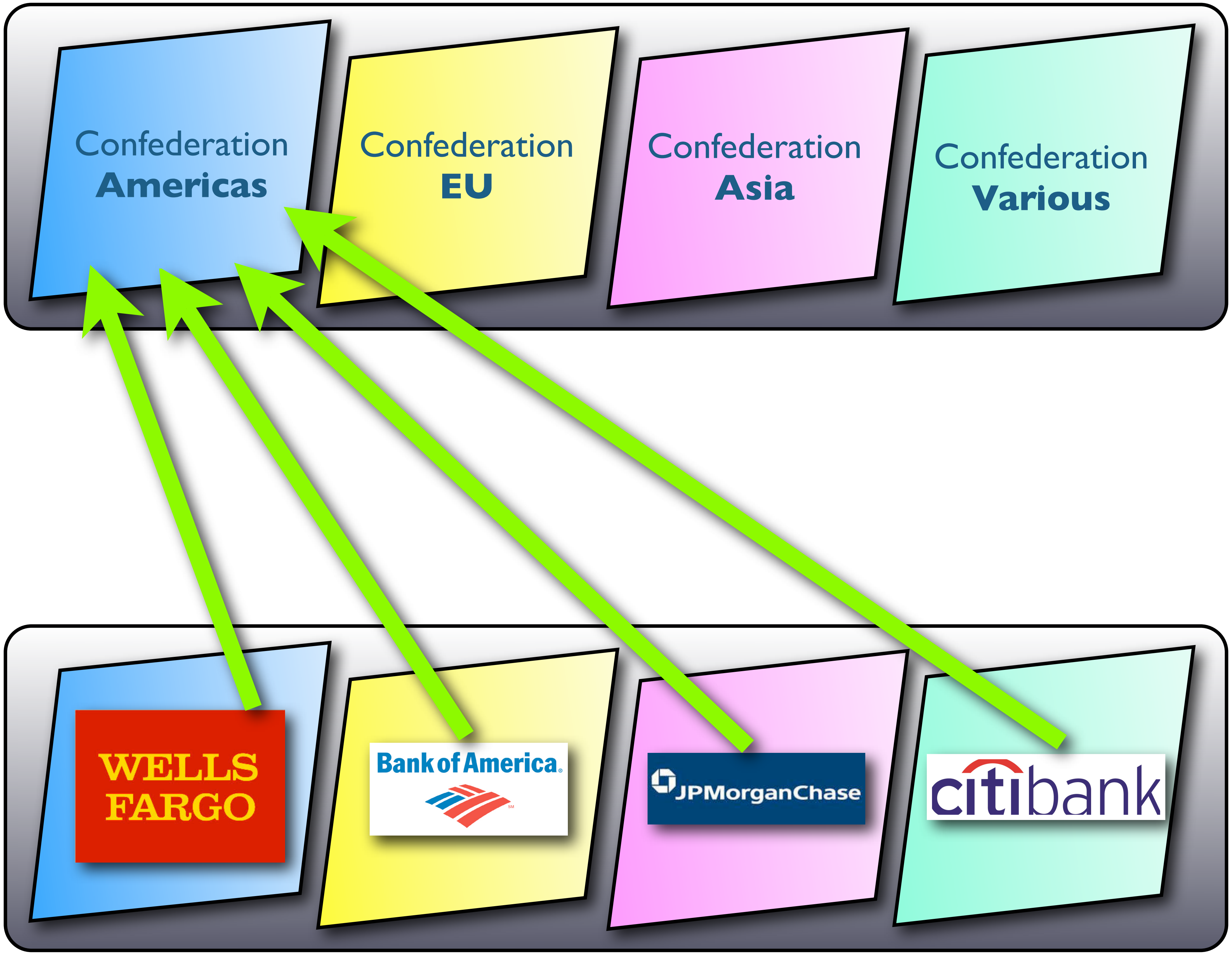
1) International

2) Regional/National

3) Sector Specific

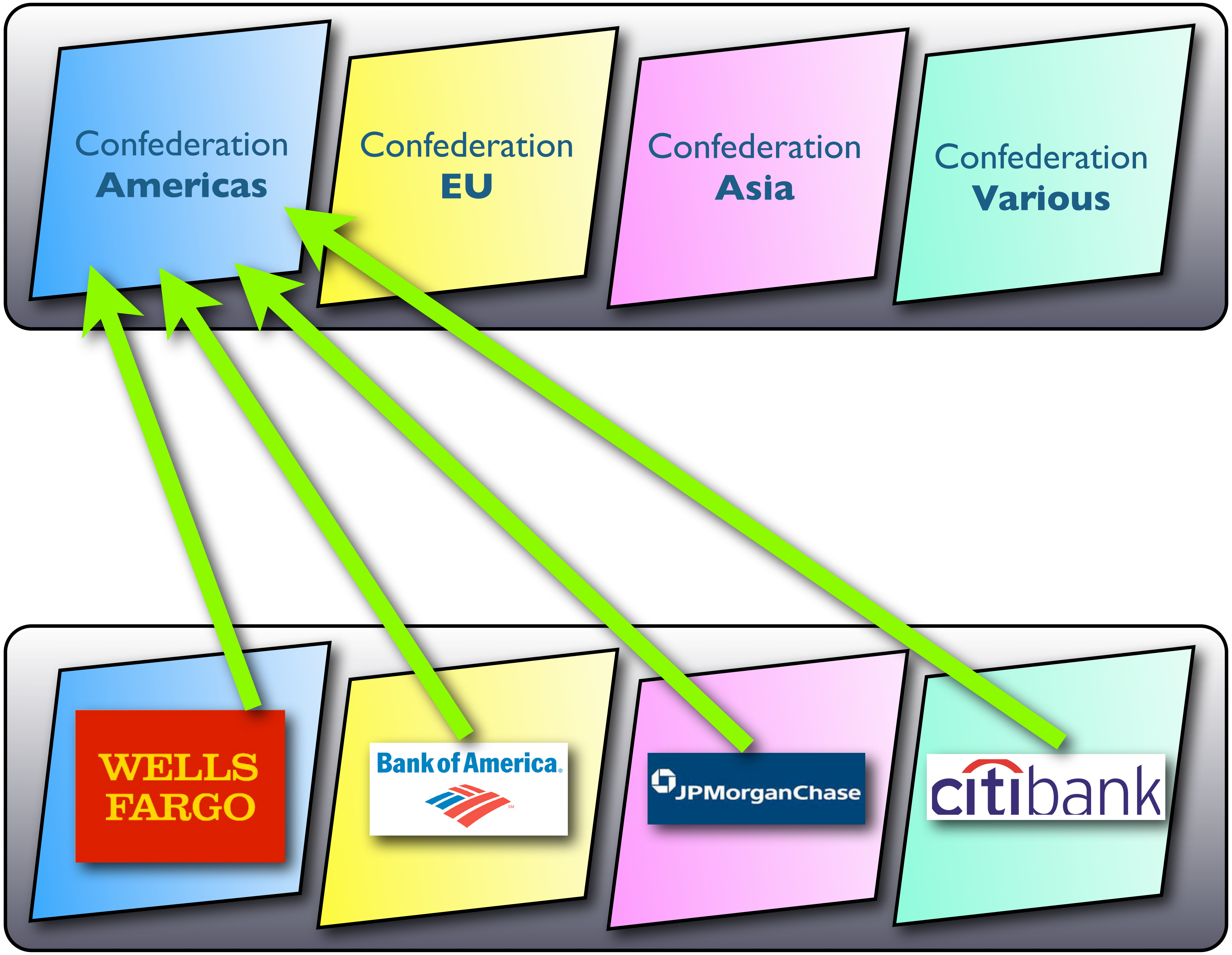


SLL: Service-providers participate in multiple systems

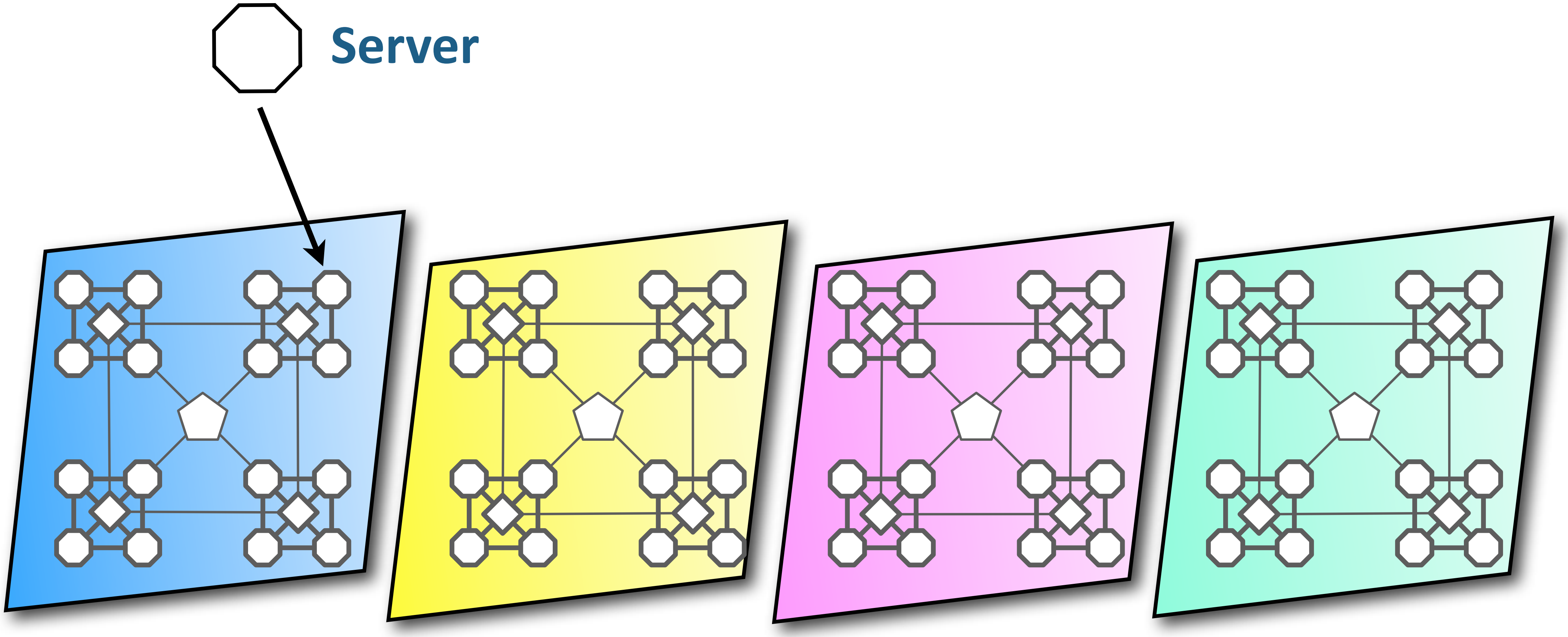


SLL: Service-providers participate in multiple systems

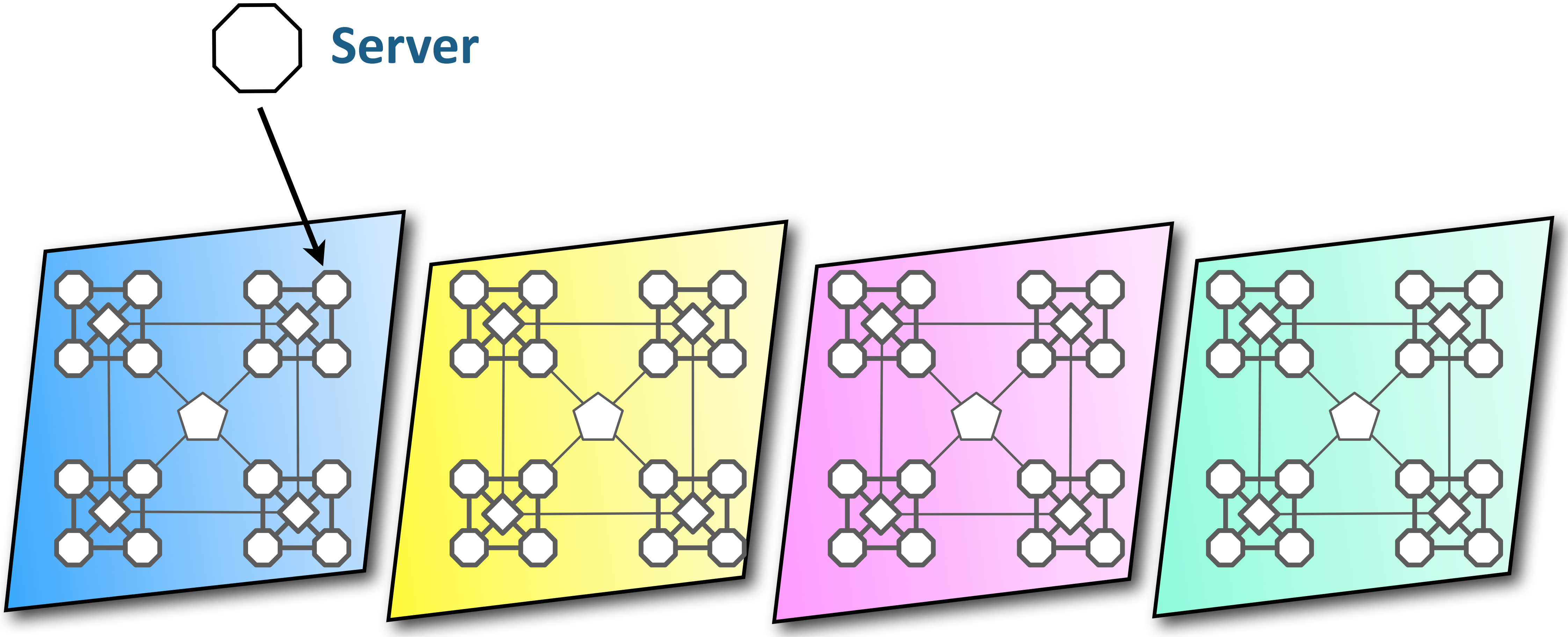
Service providers participating in a Regional, Aligned, or Sector specific system can reuse their existing infrastructure investments to participate in other systems, such as in the large international system



SLL proposal: Service providers run many servers..

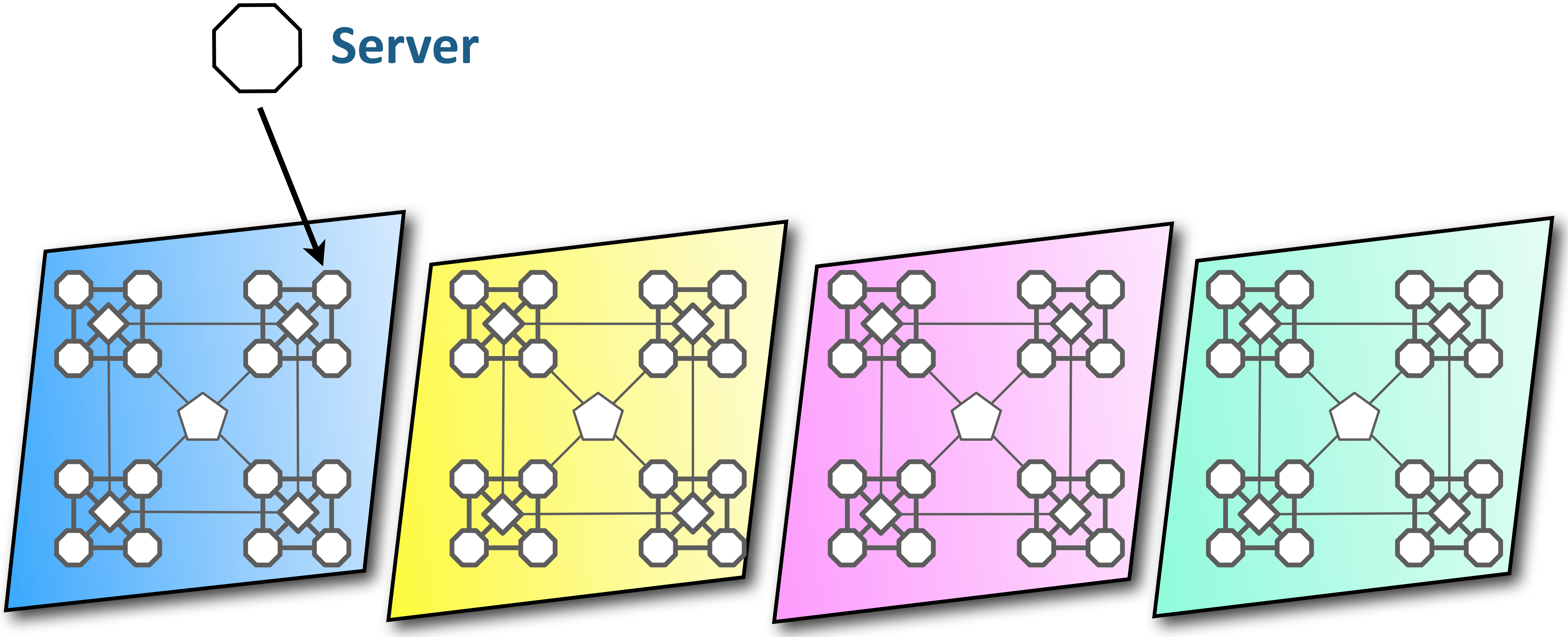


SLL proposal: Service providers run many servers..



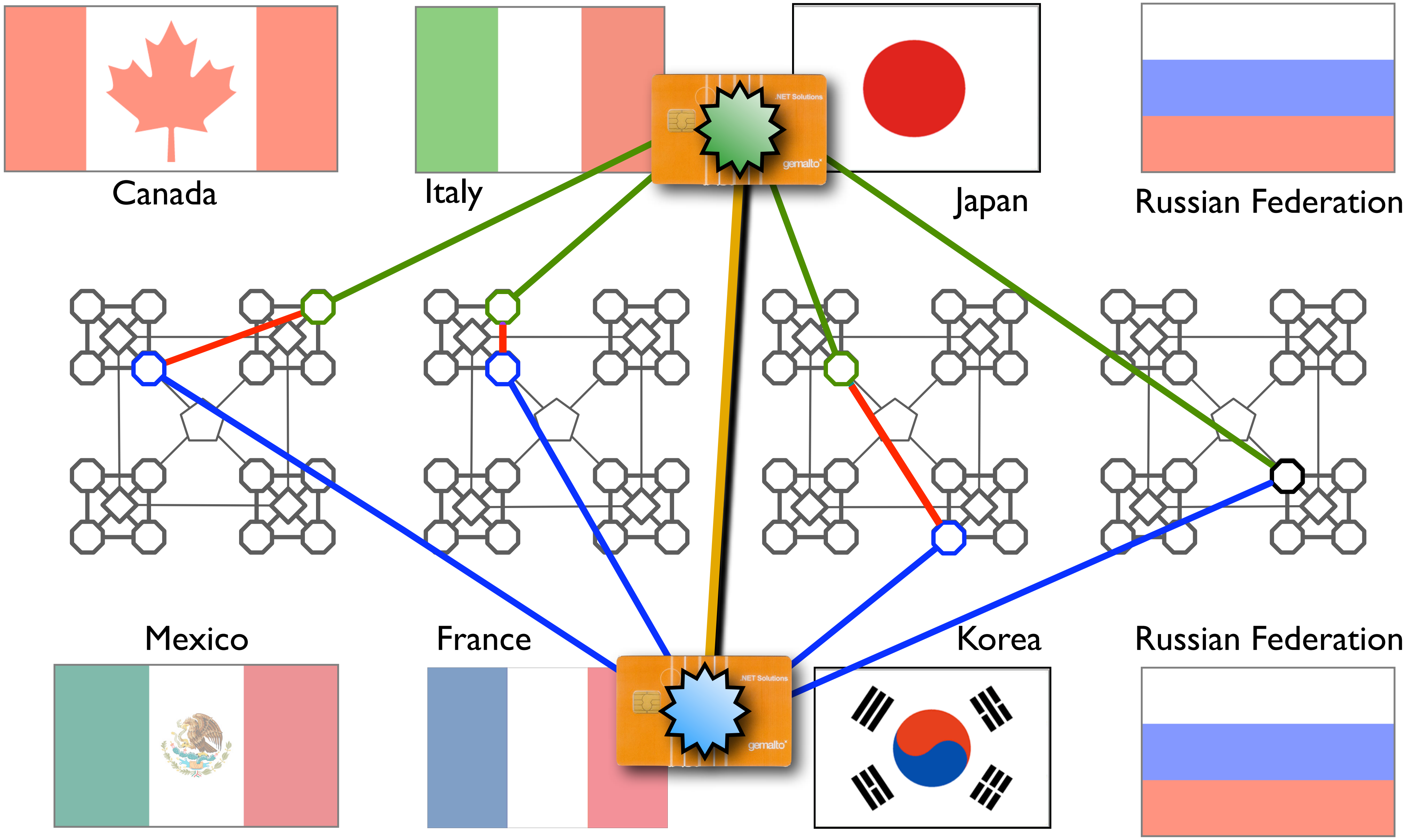
- Each organisation has many servers (4 illustrated)

SLL proposal: Service providers run many servers..



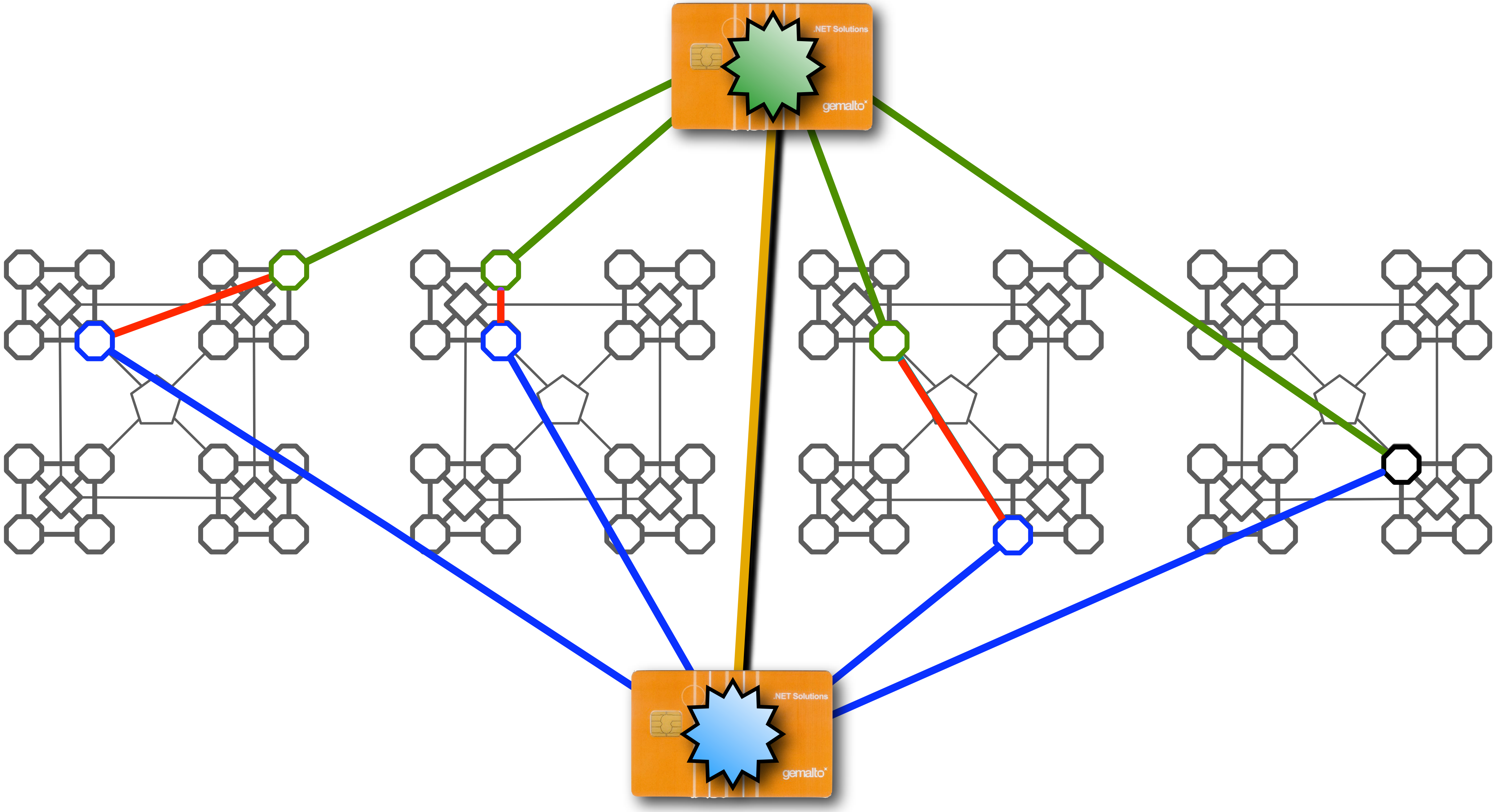
- Each organisation has many servers (4 illustrated)
  - **Each server can securely communicate within it’s confederation**

SLL: International enrolment and connectivity



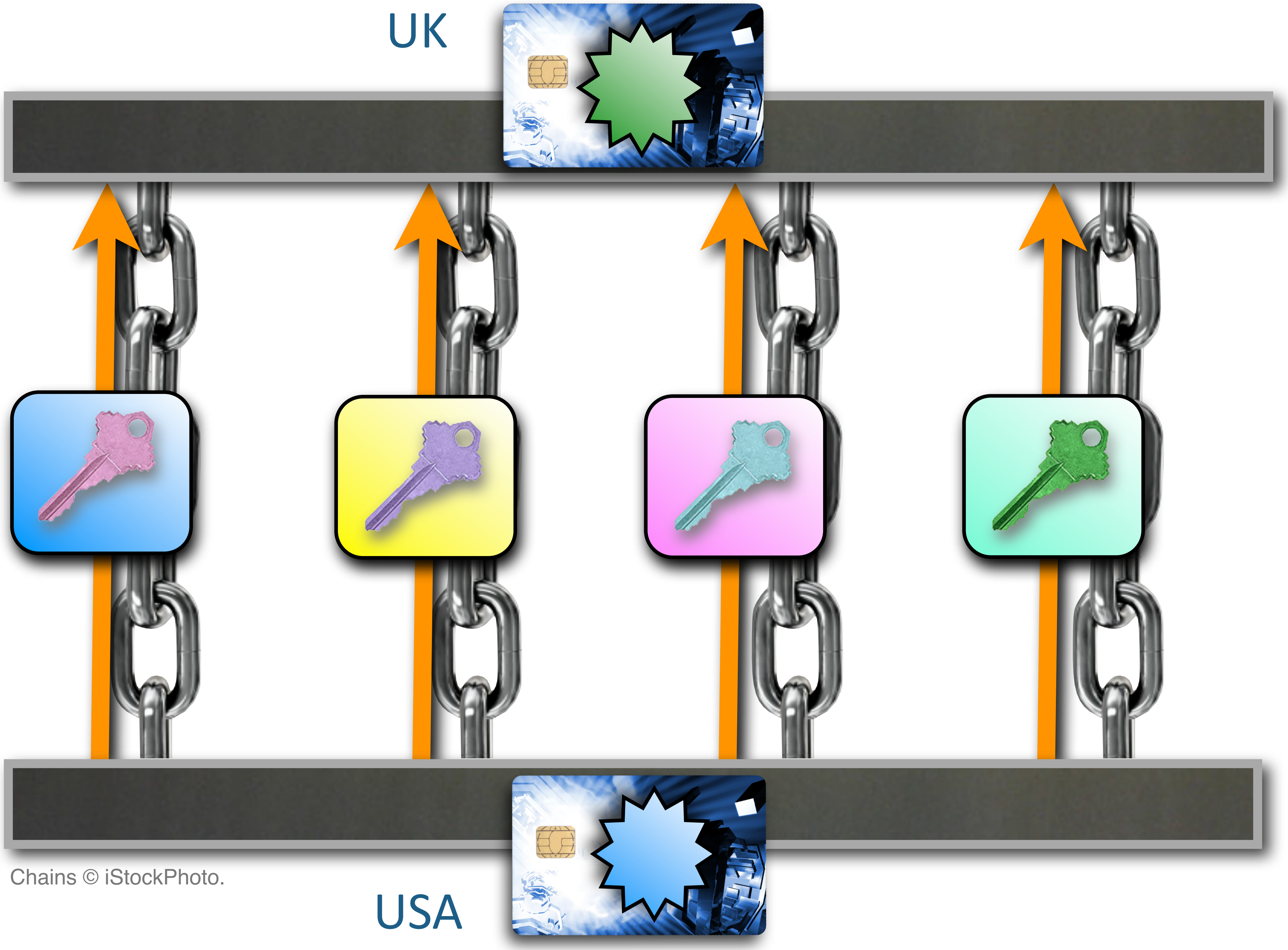
- Smart card tokens are enrolled with *m* confederations
  - any {organisation, server} pair in a confederation can be selected

SLL: Byzantine Generals' problem



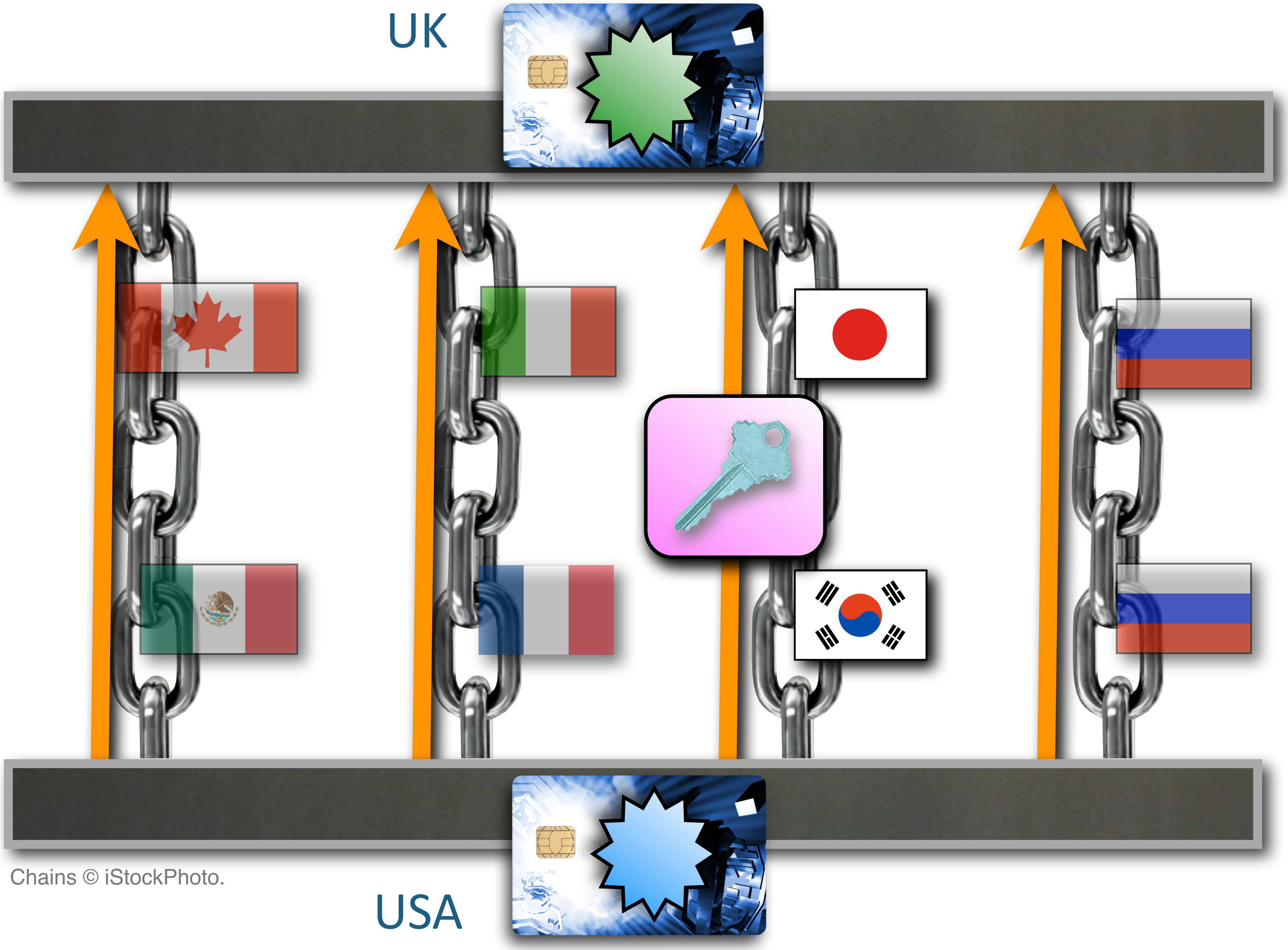
- In our scheme, we propose mapping all IdM/CKM transactions to exploit distributed, decentralised, high availability techniques

SLL: Secure key exchange between users



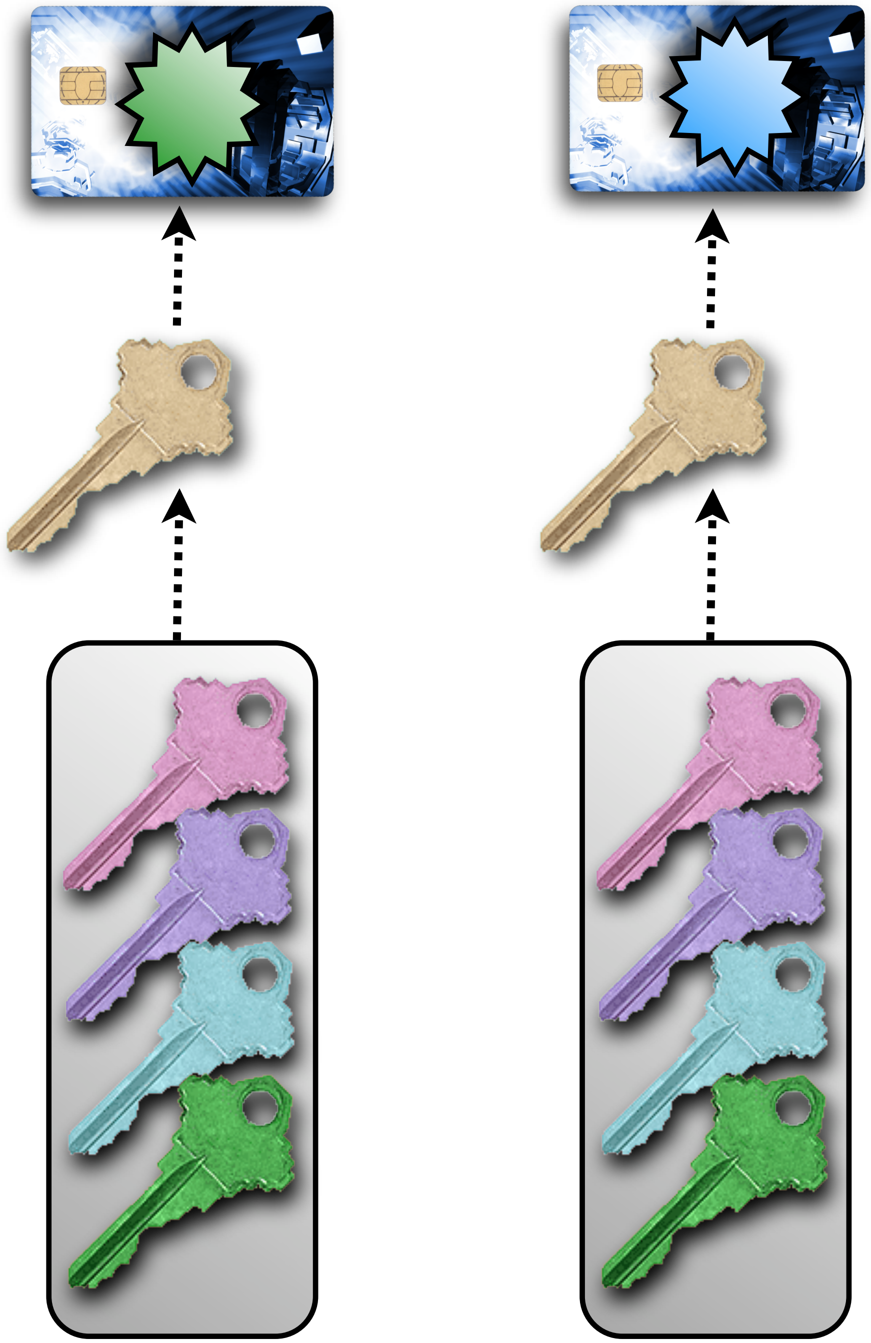
Chains © iStockPhoto.

SLL: Secure key exchange between international users



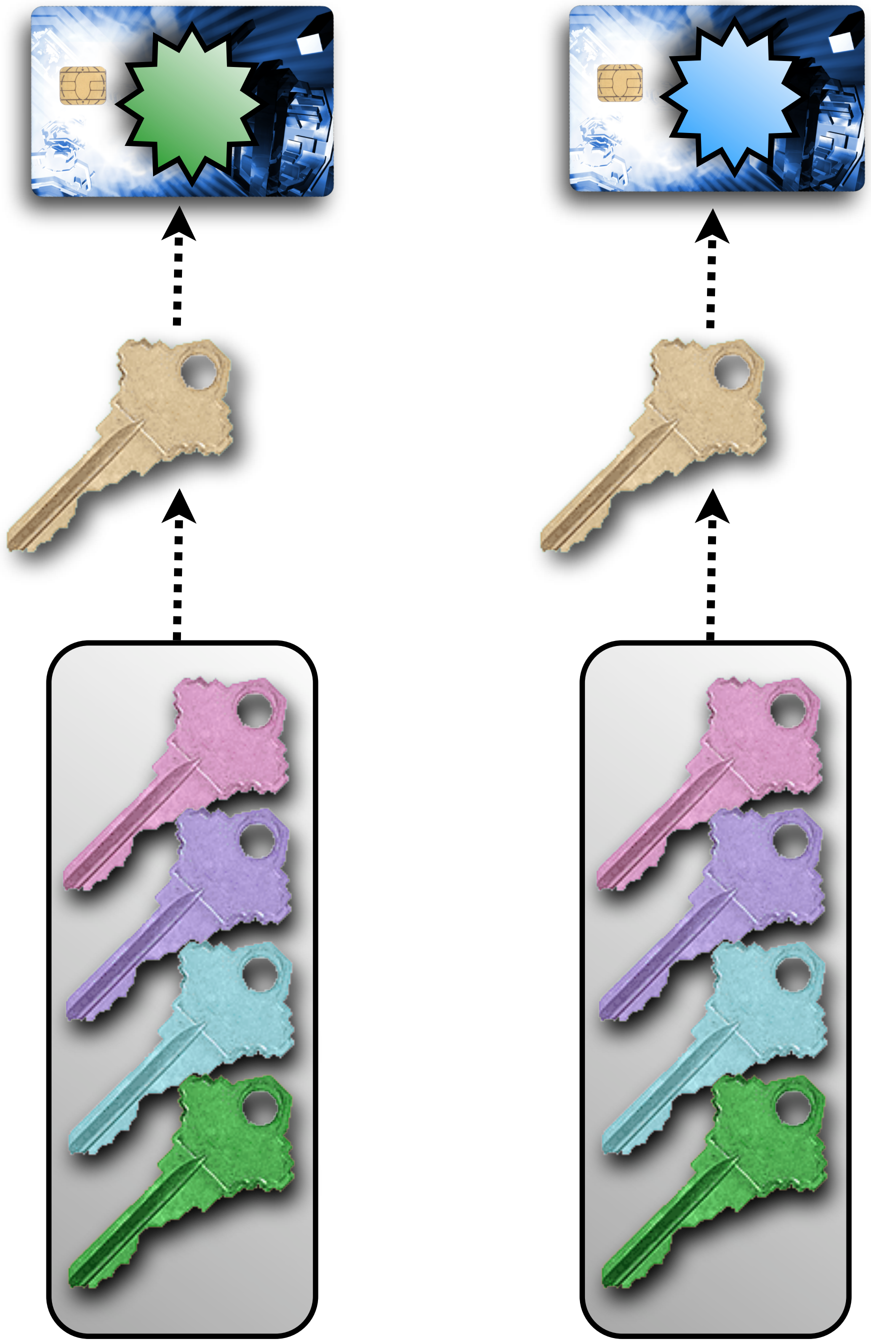
Chains © iStockPhoto.

SLL: Secure key exchange, mixing step



1. Send 4 keys over 4 distinct link-level secure relay paths

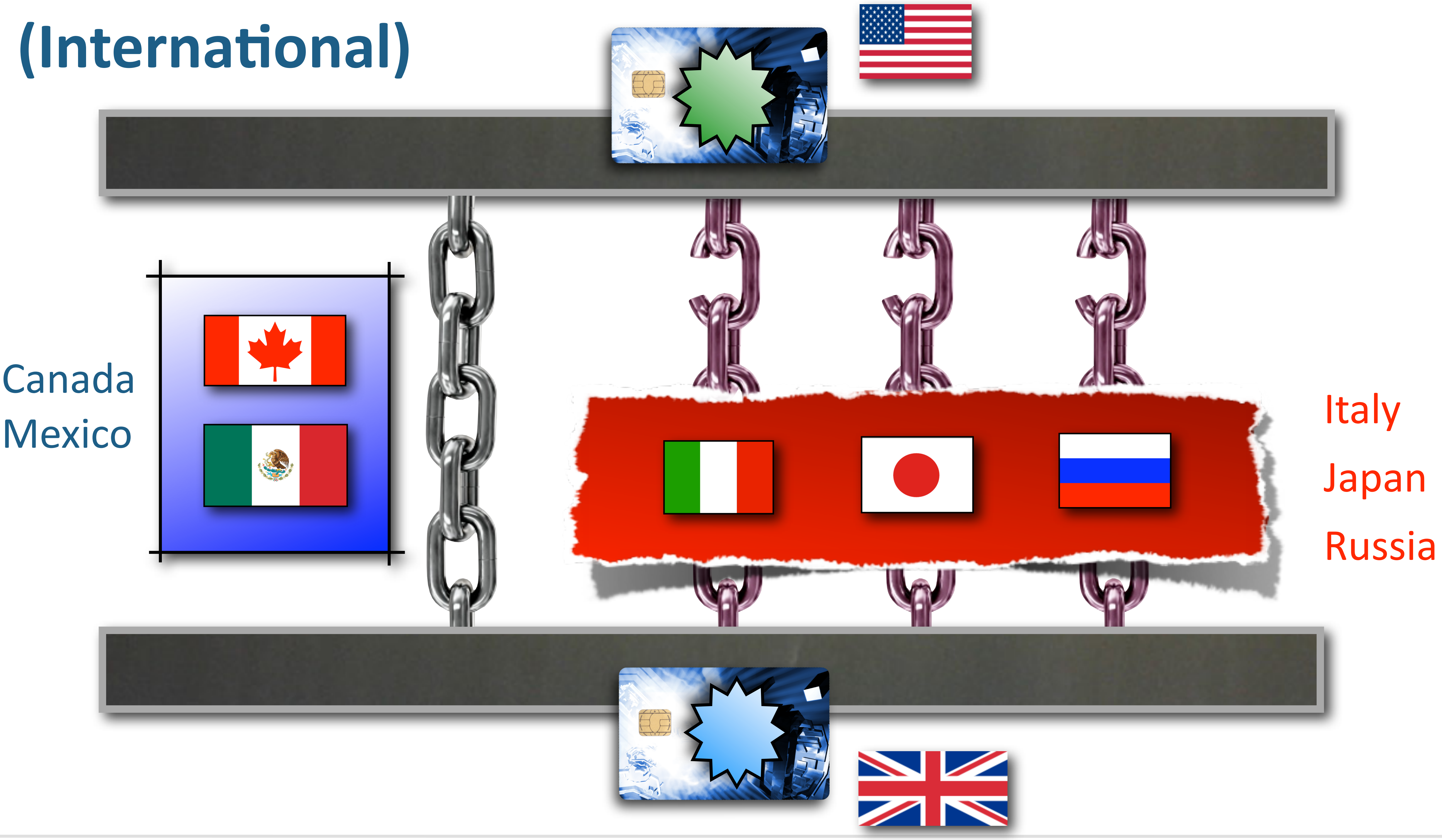
SLL: Secure key exchange, mixing step



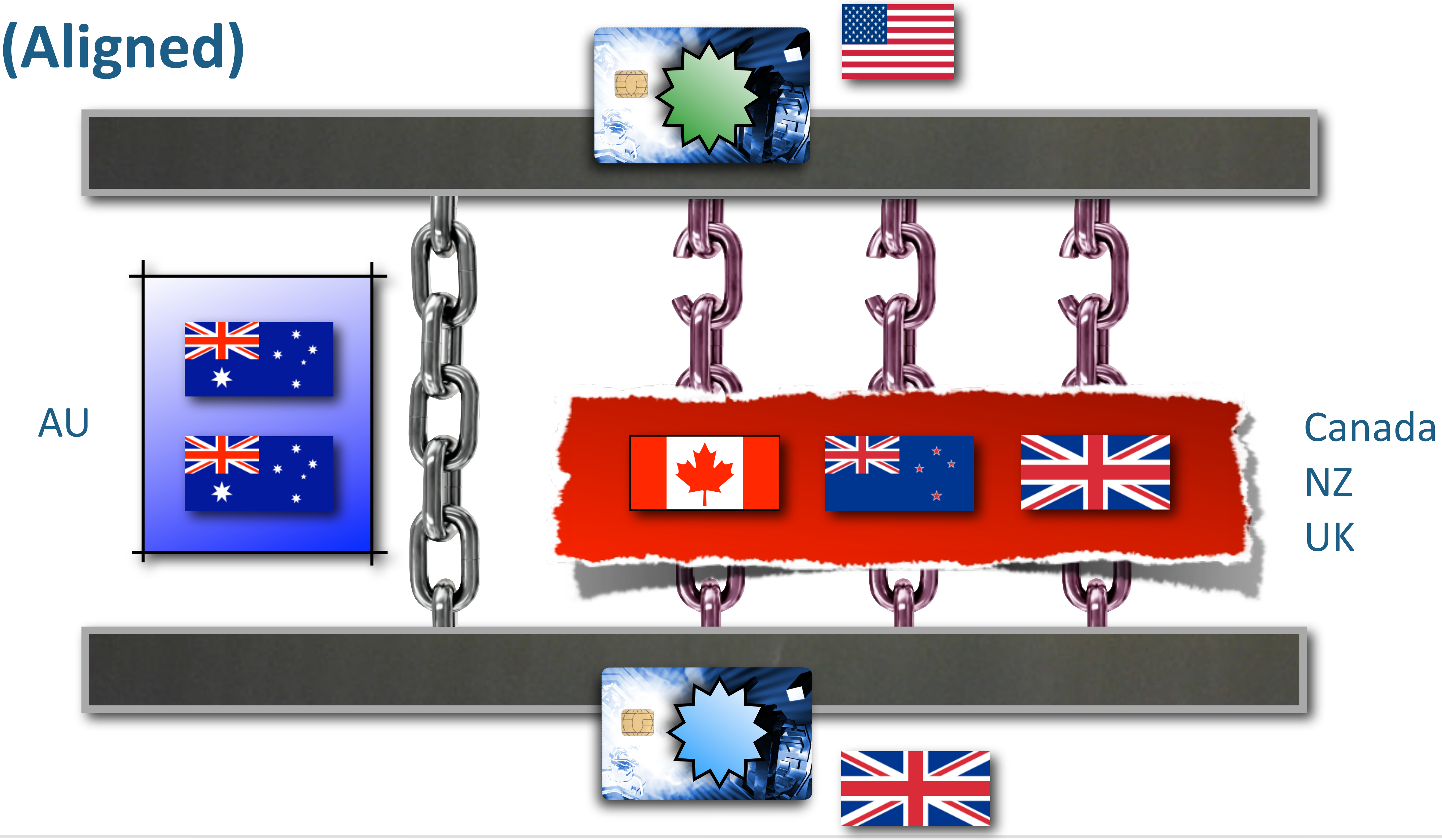
1. Send 4 keys over 4 distinct link-level secure relay paths

2. Mix/Hash 4 keys to generate master symmetric key

Fully redundant and secure against collusion (International)

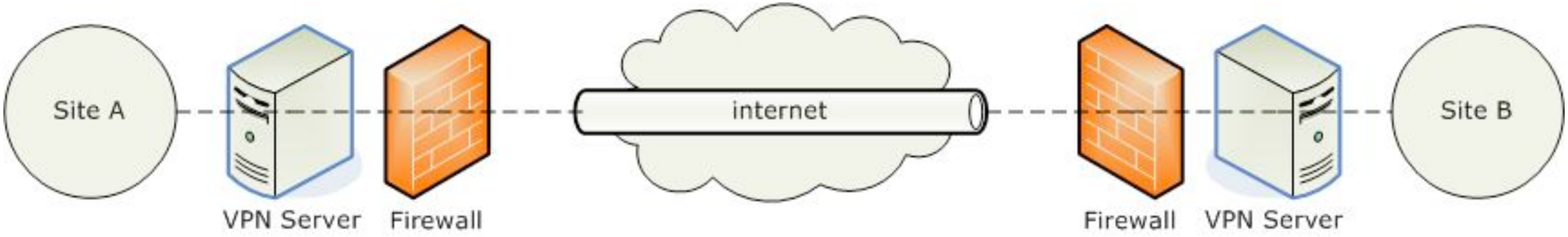


Fully redundant and secure against collusion (Aligned)



SLL proposal: VPN, tunnels, ...

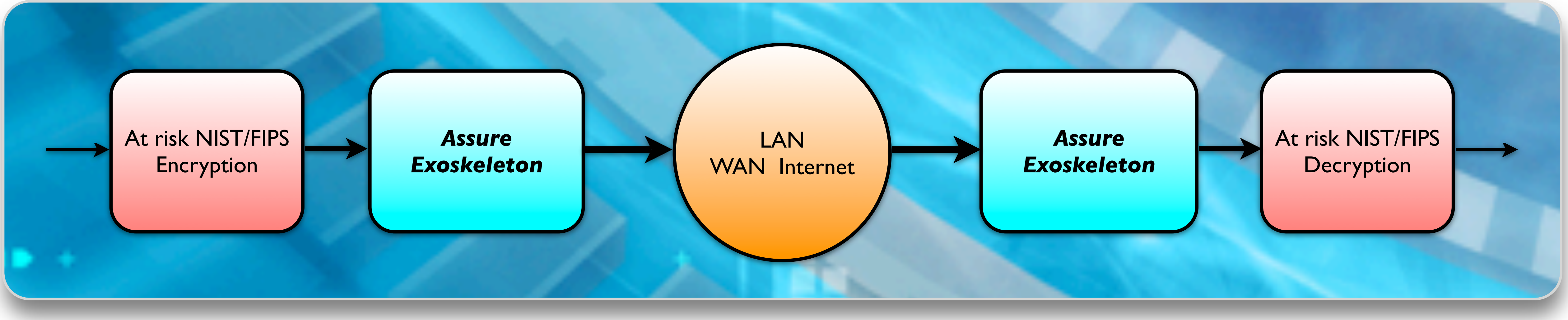
- Secure tunnels and virtual private networks (such as those offered by CISCO, Oracle, IBM, ...) are designed to easily wrap around and protect (confidentiality, integrity, authentication) the ‘at risk’ output of insecure programs without changing the programs ...



VPN image public domain from wikimedia.

SLL proposal: VPN, tunnels and Exoskeletons

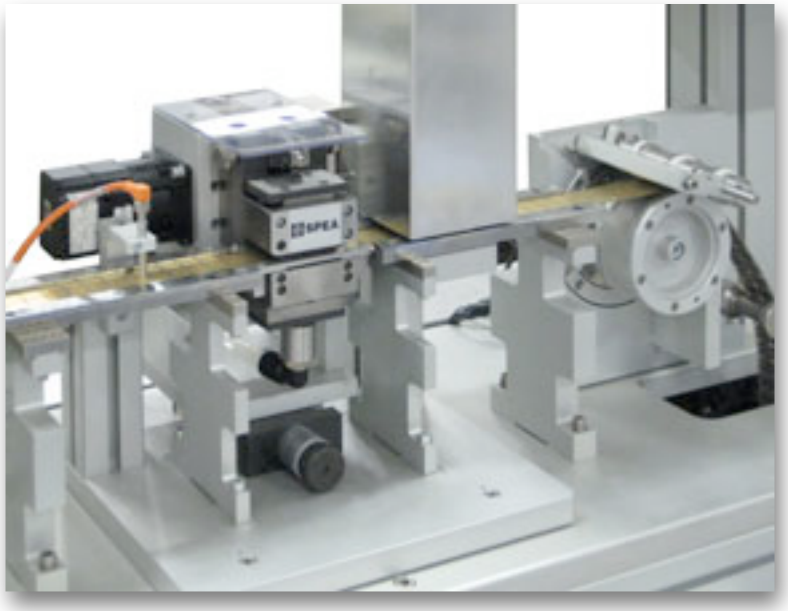
- Protocol aware secure tunnels (Exoskeletons) can easily protect the output of *individual network sessions* generated by at-risk security standards
  - No need to change protocols, or software/hardware implementations
  - Easily protect HTTP, SSL/TLS, SSL VPN, IPsec, RADIUS, SSH, ...



Background graphics © Inmagine. Used with permission.

SLL proposal: High Volume Enrolment

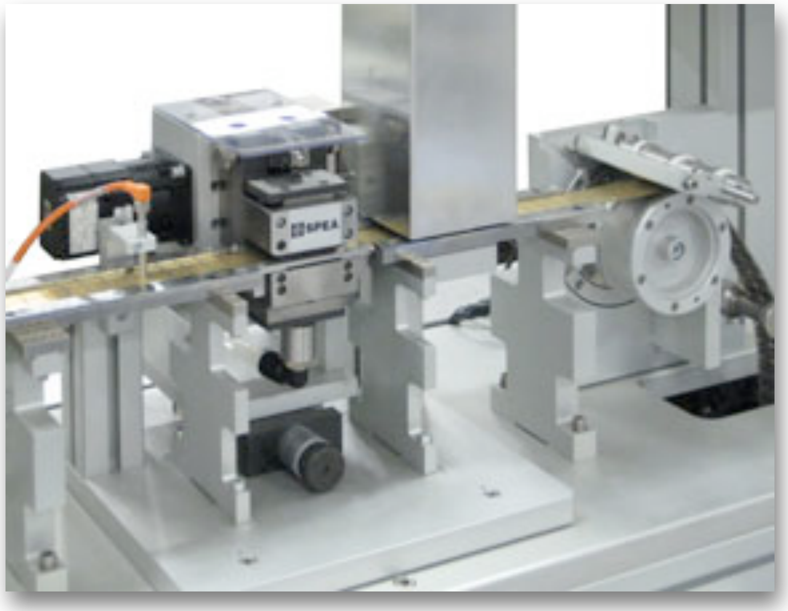
SPEA



© SPEA. Used with permission

SLL proposal: High Volume Enrolment

SPEA



- Smart card processors on reels can be programmed at rates of 1000’s of units per hour.

© SPEA. Used with permission

SLL proposal: CPU based smart cards

- **Smart cards are suitable for use as trusted couriers for symmetric keys**
- Tokens enrolled with **m** independent service providers should incrementally inject keys at **m** different locations

SLL proposal: CPU based smart cards

- **Smart cards are suitable for use as trusted couriers for symmetric keys**
- Tokens enrolled with **m** independent service providers should incrementally inject keys at **m** different locations
- Previously injected keys should **not** be read during enrolment phase (*mitigate side channel*)

SLL proposal: CPU based smart cards

- **Smart cards are suitable for use as trusted couriers for symmetric keys**

- Tokens enrolled with **m** independent service providers should incrementally inject keys at **m** different locations

- Previously injected keys should **not** be read during enrolment phase (mitigate side channel)

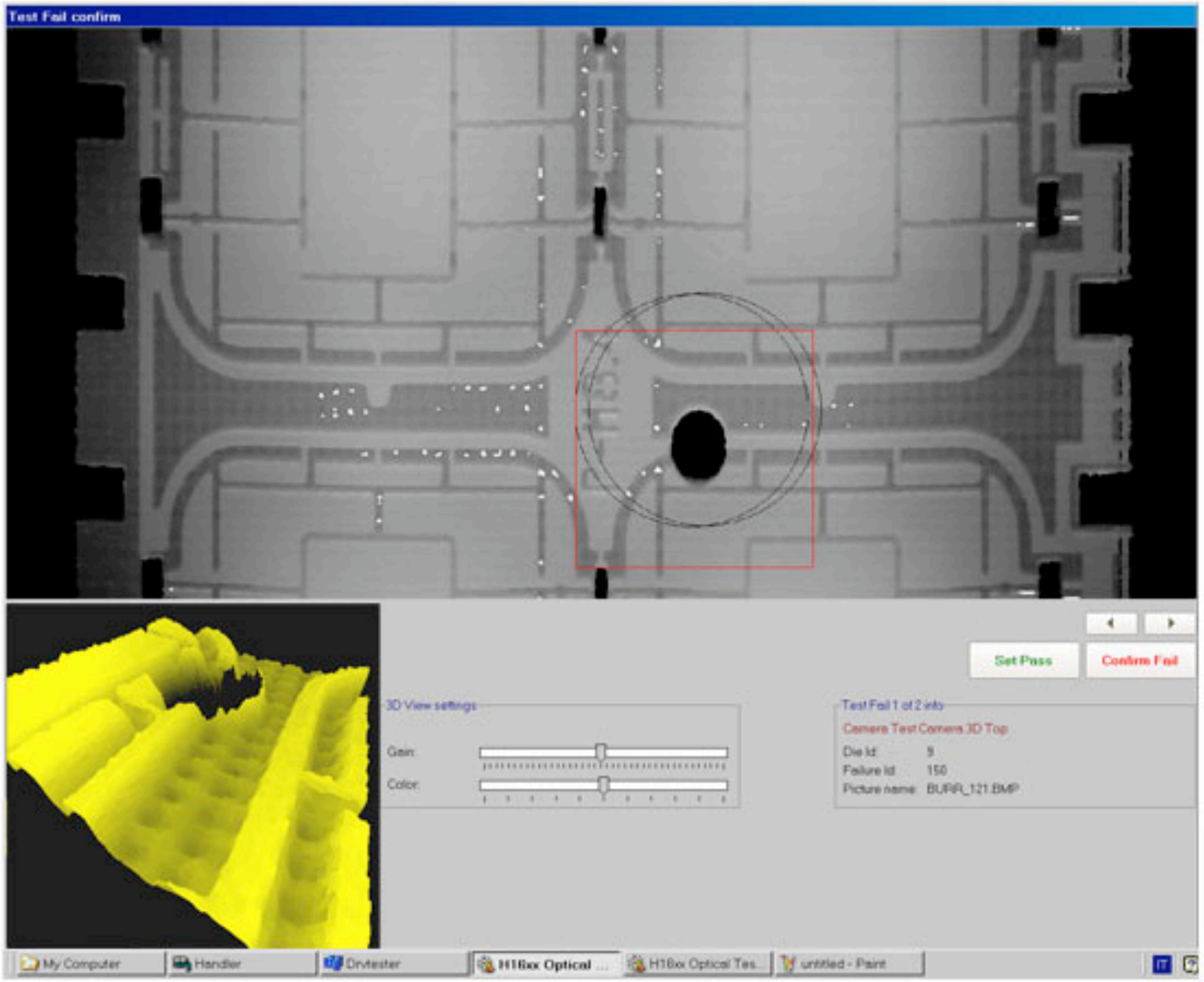
SLL proposal: CPU based smart cards

- **Smart cards are suitable for use as trusted couriers for symmetric keys**
- Tokens enrolled with **m** independent service providers should incrementally inject keys at **m** different locations
- Previously injected keys should **not** be read during enrolment phase (mitigate side channel)
- Enrolling parties may be able to *detect* suspicious behaviour before issuing cards to customers
  - Audit the # of transaction request
  - **Inspect for tampering**
  - etc

SPEA

© SPEA. Used with permission

SPEA



Test Fail 1 of 2 info

Camera Test Camera 3D Top

Die Id: 9

Failure Id: 150

Picture name: BURR_121.BMP

- In this way the system encourages openness because, while each organisation is responsible to ensure correct key injection during the phase under their control, all other participating service providers can (if they choose) observe the process and check for correctness

© SPEA. Used with permission

SLL proposal: CPU based smart cards

SLL proposal: CPU based smart cards

- **Smart cards are ideal for managing symmetric key material**
  - Symmetric operations are fast
  - Cache negotiated keys in smart card FLASH memory

SLL proposal: CPU based smart cards

- **Smart cards are ideal for managing symmetric key material**
  - Symmetric operations are fast
  - Cache negotiated keys in smart card FLASH memory

SLL proposal: CPU based smart cards

- **Smart cards are ideal for managing symmetric key material**
  - Symmetric operations are fast
  - Cache negotiated keys in smart card FLASH memory

- **If a desktop computer is compromised,**
  the token's long lived secrets are not compromised

SLL proposal: CPU based smart cards

- **Smart cards are ideal for managing symmetric key material**
  - Symmetric operations are fast
  - Cache negotiated keys in smart card FLASH memory

- **If a desktop computer is compromised,**
  the token's long lived secrets are not compromised

SLL proposal: CPU based smart cards

- **Smart cards are ideal for managing symmetric key material**
  - Symmetric operations are fast
  - Cache negotiated keys in smart card FLASH memory

- **If a desktop computer is compromised, the token's long lived secrets are not compromised**

- **Smart cards can perform forward and backwards secure key derivation**
  - Exposure of long-lived master key material from the smart-card (invasive attacks) does **not** compromise prior transactions
  - The protocol negotiates ongoing 'fresh secrets' which can protect against adversaries that discover the master key but have limited network visibility

SLL proposal: Long term confidentiality & integrity

- The SLL proposal achieves classical and post quantum security using known and trusted NIST/FIPS symmetric crypto standards. These standards have many years of study and are deployed globally, whereas today, there are no trusted post quantum secure public key algorithms.

SLL proposal: Long term confidentiality & integrity

- The SLL proposal achieves classical and post quantum security using known and trusted NIST/FIPS symmetric crypto standards. These standards have many years of study and are deployed globally, whereas today, there are no trusted post quantum secure public key algorithms.
- **NIST AES-256 is considered post quantum secure (PQS)**
  - PQS Authenticated Encryption
  - PQS Message Digests
  - Key derivation protects against related-key attacks

SLL proposal: Long term confidentiality & integrity

- The SLL proposal achieves classical and post quantum security using known and trusted NIST/FIPS symmetric crypto standards. These standards have many years of study and are deployed globally, whereas today, there are no trusted post quantum secure public key algorithms.

- **NIST AES-256 is considered post quantum secure (PQS)**
  - PQS Authenticated Encryption
  - PQS Message Digests
  - Key derivation protects against related-key attacks
  - 2AES/3AES supports >512-bit keys - may satisfy EU Call for 50-to-100 year security

SecurIST

SLL proposal: TEMPEST

SST Secure Systems & Technologies

- Electromagnetic shielding enclosures (ESE) technologies are mature and available commercially

- ESE can be used to protect the injection of symmetric keys into smart cards, <u>in a way that is resistant to</u> insider attacks

- Optionally use ESE to protect high-security service providers

© Secure Systems & Technologies Ltd. Used with permission.

SLL proposal: Platform for behavioural trust

- Online IdM/CKM systems can maintain situational awareness
- **Sonalysts Inc.** is designing a Distributed Sensor System for the Internet (Occulex) that aggregates and correlates very high-level network access behaviour **to remotely detect the presence of certain malware:**
  - Global IdM system can act as global notification system for such systems

    Detection -> Notification -> Correction -> Restoration

© Sonalysts, Used with permission.

SLL proposal: Platform for behavioural trust

- Online IdM/CKM systems can maintain situational awareness

- **Sonalysts Inc.** is designing a Distributed Sensor System for the Internet (Occulex) that aggregates and correlates very high-level network access behaviour **to remotely detect the presence of certain malware:**

  - Global IdM system can act as global notification system for such systems

    Detection -> Notification -> Correction -> Restoration

  - Joint presentation by Sonalysts and Synaptic at ORNL CSIIRW-6, 2010

© Sonalysts, Used with permission.

SLL: Enable ubiquitous IdM/CKM by identifier

- X.509 attempts to manually associate certificates with legal identities

SLL: Enable ubiquitous IdM/CKM by identifier

- X.509 attempts to manually associate certificates with legal identities
- It is much easier (for users and service providers) to associate tokens with (URI) “identifiers” that can be subject to automated challenge/response
  - e-mail accounts
  - domain names via websites, or other services

SLL: Enable ubiquitous IdM/CKM by identifier

- X.509 attempts to manually associate certificates with legal identities
- It is much easier (for users and service providers) to associate tokens with (URI) “identifiers” that can be subject to automated challenge/response
  - e-mail accounts
  - domain names via websites, or other services
- Of course, a single token can be assigned multiple identifiers.

SLL: Enable ubiquitous IdM/CKM by identifier

- X.509 attempts to <u>manually</u> associate certificates with legal identities
- It is much <u>easier</u> (for users and service providers) to associate tokens with (URI) “identifiers” that can be subject to automated challenge/response
  - e-mail accounts
  - domain names via websites, or other services
- Of course, a single token can be assigned multiple identifiers.
- Global key management through public identifiers
  - Single online clearing house
- Name spaces can be protected as national/organisational assets
  - *m* redundant lookup operations from *m* confederations

SLL: Enable ubiquitous IdM/CKM by identifier

- Identifiers can be managed to provide different levels of security

SLL: Enable ubiquitous IdM/CKM by identifier

- **Identifiers can be managed to provide different levels of security**
  - By default, ownership of an identifier is established using automated challenge/response

SLL: Enable ubiquitous IdM/CKM by identifier

- **Identifiers can be managed to provide different levels of security**
  - By default, ownership of an identifier is established using automated challenge/response
    - billions of enrolled identifiers

SLL: Enable ubiquitous IdM/CKM by identifier

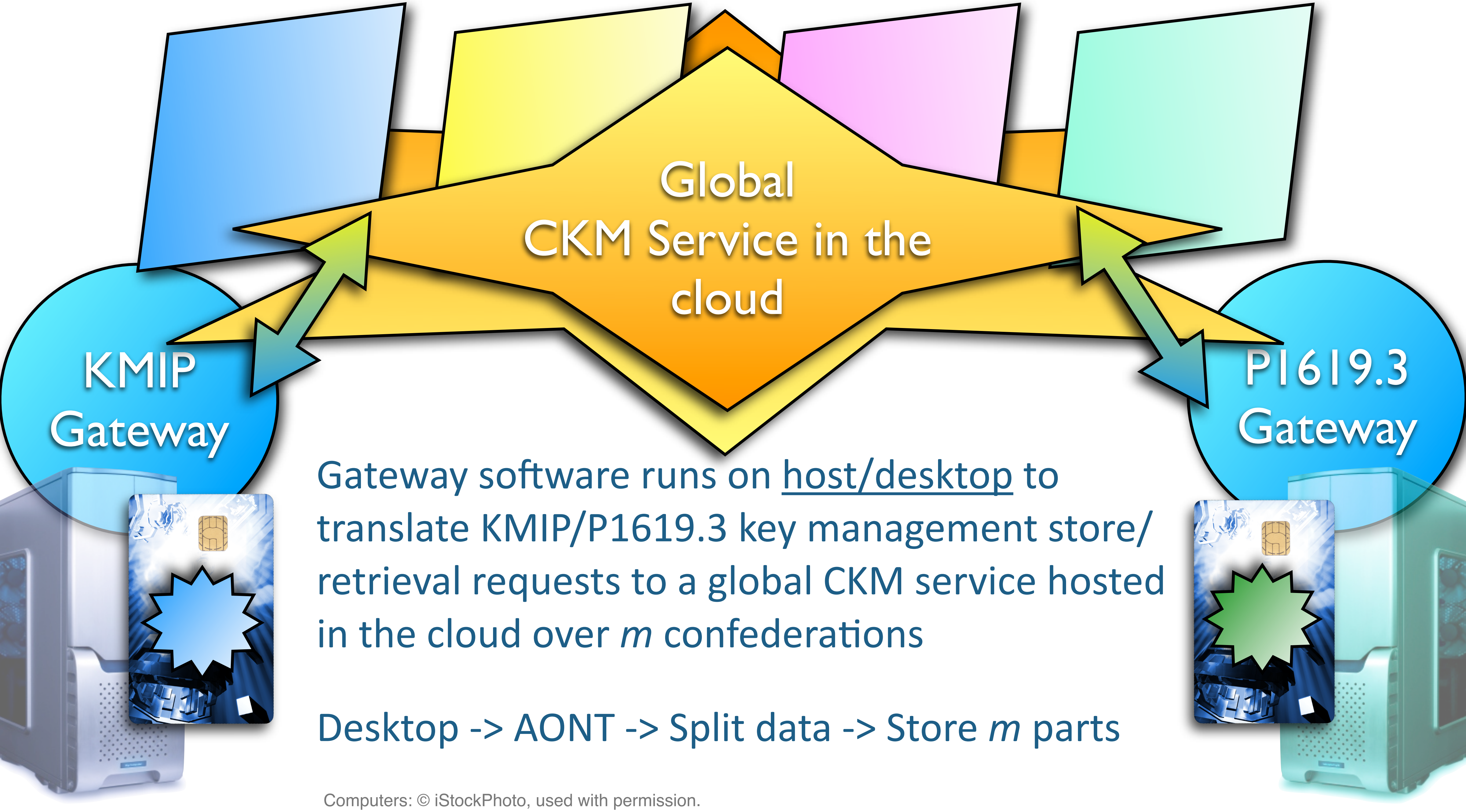
- **Identifiers can be managed to provide different levels of security**
    - By default, ownership of an identifier is established using automated challenge/response
        - billions of enrolled identifiers
    - Increased control/assurance through certificate-authority mechanisms
        - “human in the loop”
        - millions of enrolled identifiers

SLL proposal: Online validation

- Real-time online validation of identifiers and tokens costs less money (CPU time) when symmetric techniques are used
  - Exploit existing pre-shared secrets for message integrity (MAC)
  - NO $$$ DIGITAL SIGNATURES

- Online IdM/CKM can optionally maintain relationship histories between **tokens** to facilitate “push based” revocation notification
  - Precision notification based on existing relationship
  - Reduce need for “POLL” driven architectures

SLL proposal: (*m*-1) secure interoperable CKM



Gateway software runs on host/desktop to translate KMIP/P1619.3 key management store/ retrieval requests to a global CKM service hosted in the cloud over *m* confederations

Desktop -> AONT -> Split data -> Store *m* parts

Computers: © iStockPhoto, used with permission.

Conclusions

- **PKI systems originally designed for offline operation are now ONLINE**
  - Symmetric ID systems are more efficient than offline digital signatures

Conclusions

- **PKI systems originally designed for offline operation are now ONLINE**
  - Symmetric ID systems are more efficient than offline digital signatures
- **X.509 PKI has multiple single point of trust failures**
  - Symmetric ID systems can protect against insider and outsider attacks

Summary of the current environment

- **PKI systems originally designed for offline operation are now ONLINE**
  - Symmetric ID systems are more efficient than offline digital signatures
- **X.509 PKI has multiple single point of trust failures**
  - Symmetric ID systems can protect against insider and outsider attacks

Summary of the current environment

- **PKI systems originally designed for offline operation are now ONLINE**
  - Symmetric ID systems are more efficient than offline digital signatures
- **X.509 PKI has multiple single point of trust failures**
  - Symmetric ID systems can protect against insider and outsider attacks
- **There is no backwards security if a PKC system is compromised**
  - Symmetric systems can achieve both backwards and forwards secrecy

Summary of the current environment

- **PKI systems originally designed for offline operation are now ONLINE**
  - Symmetric ID systems are more efficient than offline digital signatures
- **X.509 PKI has multiple single point of trust failures**
  - Symmetric ID systems can protect against insider and outsider attacks
- **There is no backwards security if a PKC system is compromised**
  - Symmetric systems can achieve both backwards and forwards secrecy
- **In 2009 NIST has called for symmetric CKM solutions**
  - robustness, availability, and accountability
  - scalability to billions of users
  - interoperability

We have proposed a new IdM/CKM design that:

- **relies only on symmetric techniques to achieve post quantum security**
  - leverages commodity smart cards for key management
  - uses electromagnetic shielded enclosures to protect PSK injection

We have proposed a new IdM/CKM design that:

- **relies only on symmetric techniques to achieve post quantum security**
  - leverages commodity smart cards for key management
  - uses electromagnetic shielded enclosures to protect PSK injection
- **is massively scalable wrt to:**
  - number of (international) service providers
  - number of (international) users

We have proposed a new IdM/CKM design that:

- **relies only on symmetric techniques to achieve post quantum security**
  - leverages commodity smart cards for key management
  - uses electromagnetic shielded enclosures to protect PSK injection
- **is massively scalable wrt to:**
  - number of (international) service providers
  - number of (international) users
- **does not have “system-wide” single point of trust failure**
  - protects name spaces as assets of respective owners
  - support accountability and transparency

We have proposed a new IdM/CKM design that:

- **Supports “tailored trustworthy spaces” (NITRD)**
  - Tailored mapping of services providers to reflect different systems of confederation mappings to reflect different trust models
  - Tailored levels of security wrt to identifier assertions in global system

We have proposed a new IdM/CKM design that:

- **Supports "tailored trustworthy spaces" (NITRD)**
  - Tailored mapping of services providers to reflect different systems of confederation mappings to reflect different trust models
  - Tailored levels of security wrt to identifier assertions in global system
- **Supports "Moving Target" theme (NITRD)**
  - Forwards and backwards secrecy (value of symmetric keys evolve)
  - Dynamic challenge/response authentication (Not username, password)

We have proposed a new IdM/CKM design that:

- **Supports "tailored trustworthy spaces" (NITRD)**
  - Tailored mapping of services providers to reflect different systems of confederation mappings to reflect different trust models
  - Tailored levels of security wrt to identifier assertions in global system
- **Supports "Moving Target" theme (NITRD)**
  - Forwards and backwards secrecy (value of symmetric keys evolve)
  - Dynamic challenge/response authentication (Not username, password)
- **Can be used to wrap-around and protect existing PKI based systems**

We have proposed a new IdM/CKM design that:

- **Supports "tailored trustworthy spaces" (NITRD)**
  - Tailored mapping of services providers to reflect different systems of confederation mappings to reflect different trust models
  - Tailored levels of security wrt to identifier assertions in global system
- **Supports "Moving Target" theme (NITRD)**
  - Forwards and backwards secrecy (value of symmetric keys evolve)
  - Dynamic challenge/response authentication (Not username, password)
- **Can be used to wrap-around and protect existing PKI based systems**
- **Can be adapted to provide an inter-operable (Global) Enterprise Key Management solution**

We have proposed a new IdM/CKM design that:

- **Supports "tailored trustworthy spaces" (NITRD)**
  - Tailored mapping of services providers to reflect different systems of confederation mappings to reflect different trust models
  - Tailored levels of security wrt to identifier assertions in global system
- **Supports "Moving Target" theme (NITRD)**
  - Forwards and backwards secrecy (value of symmetric keys evolve)
  - Dynamic challenge/response authentication (Not username, password)
- **Can be used to wrap-around and protect existing PKI based systems**
- **Can be adapted to provide an inter-operable (Global) Enterprise Key Management solution**
- **Can be adapted to support various behavioural trust models**

Collaboration:

Collaboration:

- Currently approximately 12 international corporations, interested to assist with development, each specialising in some aspect or element of the Synaptic proposal and its end-user applications

Collaboration:

- Currently approximately 12 international corporations, interested to assist with development, each specialising in some aspect or element of the Synaptic proposal and its end-user applications

- Calling for additional US and international collaborators

Collaboration:

- Currently approximately 12 international corporations, interested to assist with development, each specialising in some aspect or element of the Synaptic proposal and its end-user applications
  - NATO approved SST (UK) for TEMPEST
  - NCP-e (German) for Virtual Private Networks
  - Secure Shell Limited (Finland) for SSH
  - Quintessence Labs (Australia) for QKD
  - Sonalysts (USA) for network behavioral security
  - Tesacom (Latin America) for satellite communications.
- Calling for additional US and international collaborators
  - Marketing strategy and partner for a major region now advancing, targeting large corporations (including within world's top 10)

Architecture and collaborator enquiries:

Benjamin GITTINS

CTO and System Architect
Synaptic Laboratories Limited

Email:	cto@pqs.io
Phone:	+356 2701 9390
Web:	http://pqs.io