



Personal identity solution for the corporate-to-bank space

Martine Boutineau, Société Générale

Elie Lasker, SWIFT

Willy Verhanneman, SWIFT

Background

- **2004:** SWIFT for Corporates - requirement of personal signature emerges in France
- **Mid 2007:** Corporate Advisory Group (CAG) requests SWIFT to investigate possible approaches
- **Q4 2007 – End 2008:** workshops with working group to investigate possible solutions
- **June 2009:** Board approves building of proposed solution



Sept 17th 2009



Photos: Patrick Messina / Metis

Personal identity in the corporate-to-bank space

Sibos 2009 – Hong Kong



SOCIETE GENERALE
Payment Services



Personal identity: Which drivers ?

- **A major responsibility for the bank :**
 - ensure that the instruction can be securely and legitimately acted upon
 - ➔ In many countries, a legal entity can act only through individuals, duly empowered as representatives

- **An additional service to corporates :**
 - delegation to the bank of the checking of all signatures' entitlements Vs the channel used , the type of the orders issued, the amounts involved,
 - ➔ Can only be achieved relying on signatures by each and every individual

- **An increasingly restrictive legal environment**
 - Basel 2, AML laws, Sarbanes Oxley in the US, decisions from central banks and other local authorities
 - ➔ Need for transaction tracking end to end, and proof archiving capabilities ...

- **A Growing demand to extend the scope of dematerialization**
 - ▶ Archiving, guarantees issuance, financing solutions, bank account management (signatories updates, additional account opening...)...

= Drivers for non repudiation at individual level

- **Actual Electronic signature is mainly based on PKI systems**
- **The related keys can be previously exchanged between partners, or included in certificates**
- **A large majority of signing solutions are now certificate based, particularly X509 ones**
- **To be acted upon by the recipient, the data must be signed :**
 - ▶ Using an expected signing method
 - ▶ With a certificate the recipient can operate and is willing to accept
- ➔ **What's needed ?**
 - Recognition of e signing as legally binding
 - Standards to be operable in more than one bank
 - Confidence to be widely accepted

Recognition of e signing as legally binding

- **Depends on the governing law of each country**
 - ▶ Now effective in a large number of countries
 - ▶ Relatively easy to implement and use in most jurisdictions if governed by contract law (e.g. electronic banking)

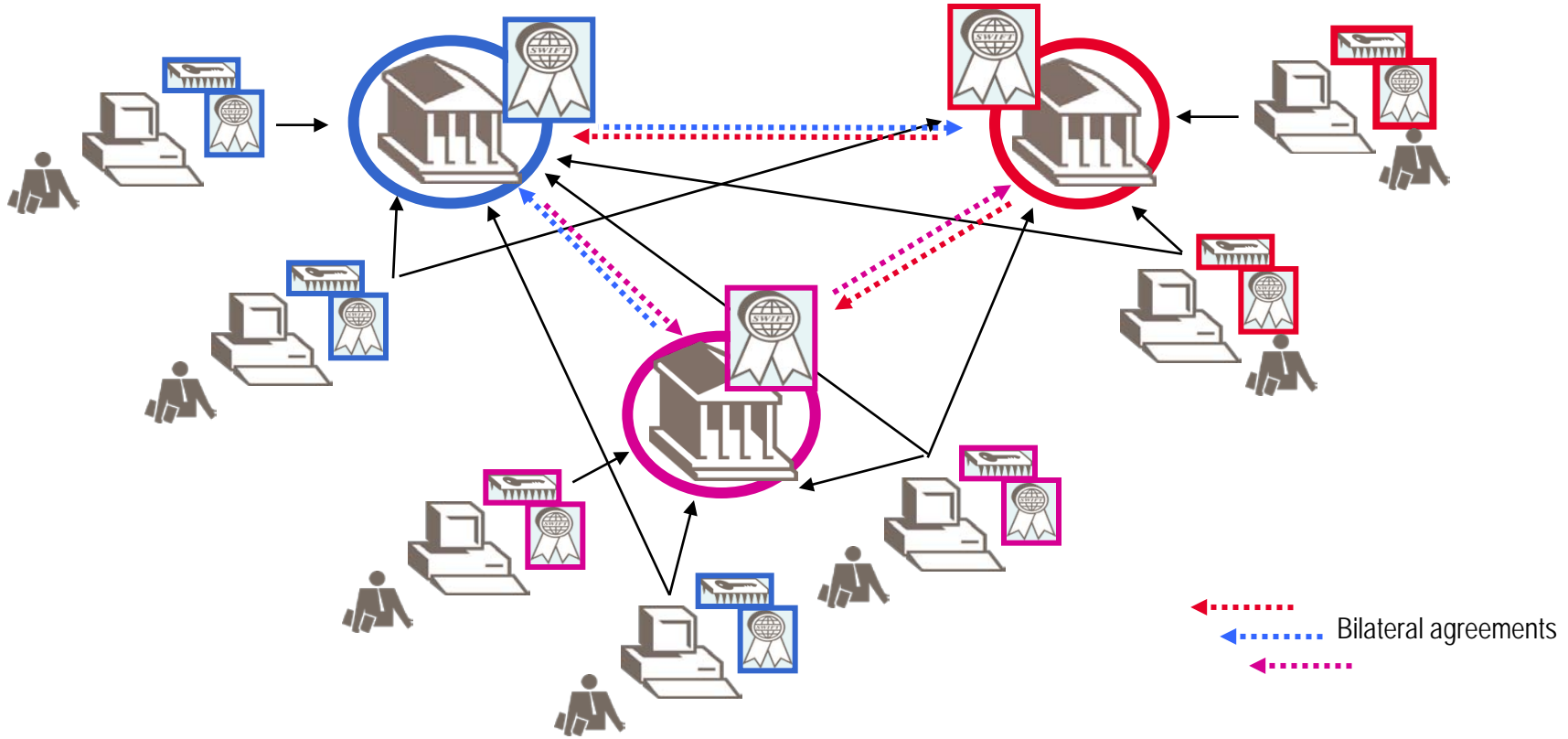
Standards, to be interoperable

- **Even a standard like X 509 lets room for interpretations**
- **An illustration : use in France**
 - ▶ A solution launched by government bodies for VAT declaration and payment
 - ▶ Much time lost to agree on a common implementation method
 - ▶ Additional delay to issue common signing practices

Confidence, to be widely accepted

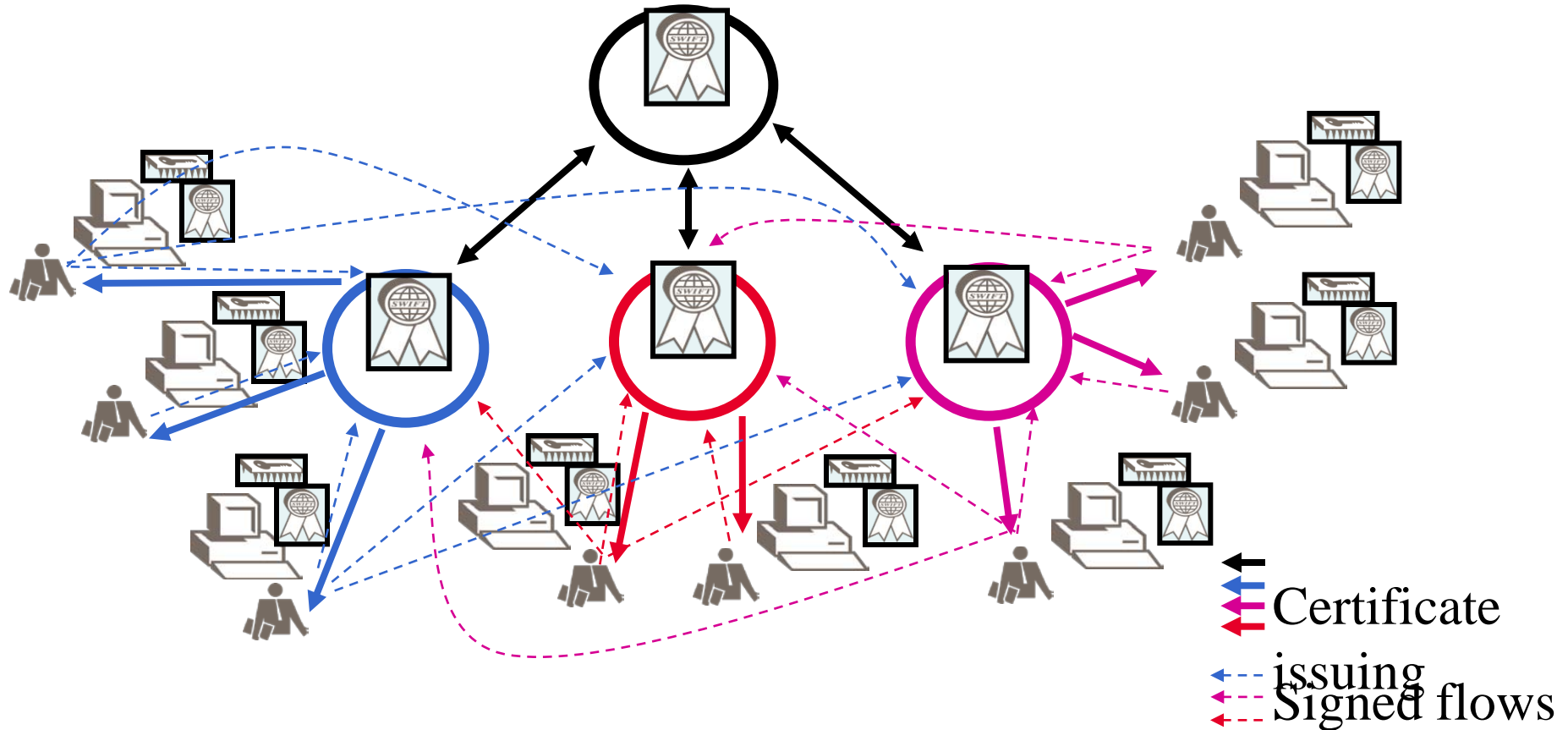
- **Reliance on the technical quality of the solution and**
- **On the security of the registration**

Possible schemes: option 1 , Bilateral



heavy, complicated,
use probably restricted to arrangements within a same local
geographical area
doesn't necessarily provide for common signing method

Possible schemes: option 2 , Hierarchical



All certificates issued by any of the Certification Authorities (CA) operating in the model must be accepted,
Single registration (by issuing Bank),
Security relies on the respect by all actors of the rules prescribed for issuing and registration,
Doesn't deal with signing methods

- **A certificate standard at international level**
- **Independent from file format**
- **Usable in different exchange environments (File transfer solutions such as File Act, authentication and signing over internet...)**
- **Providing for multi acceptance , respectful of some banks wish to master their own registration process**
- **Adding possible use of a standard signing method , whether included in the solution or for integration by vendors**
- **As much in line as possible with already existing solutions to limit additional investments**
- **Processed within a reliable organisation**

Principles of proposed solution

- SWIFT provides PKI certificates usable by corporate representatives, but not identifying a specific owner
- Usable to sign in a non-repudiable manner
- Effective only if registered (associated with a corporate representative) by each bank separately

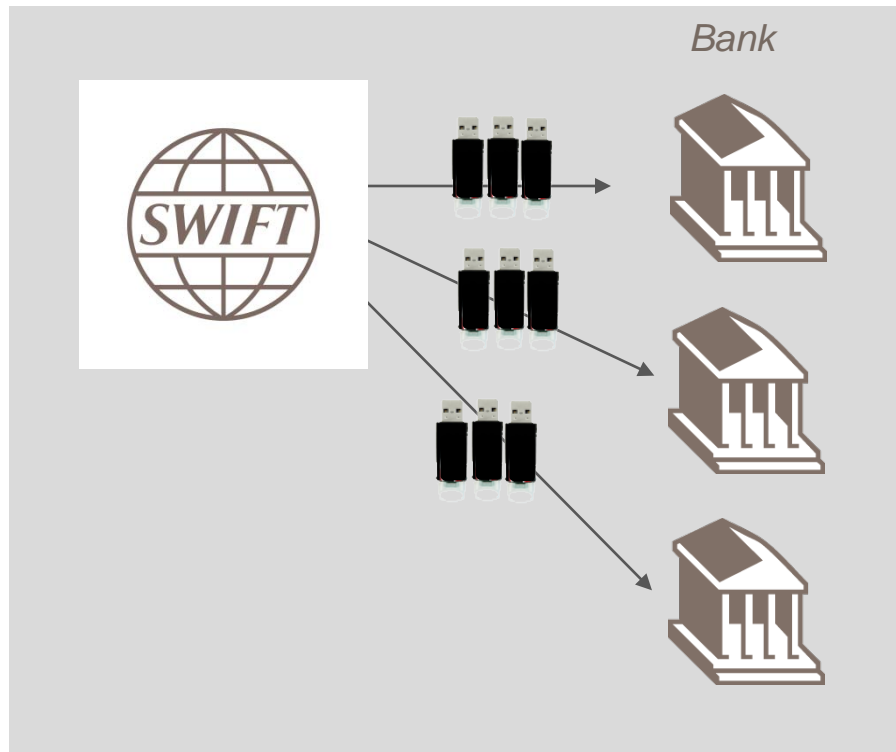
Solution can be used over SWIFTNet and Internet



Overview of proposed solution

Step 1: SWIFT ships inactive tokens to banks

Participating banks receive a set of tokens



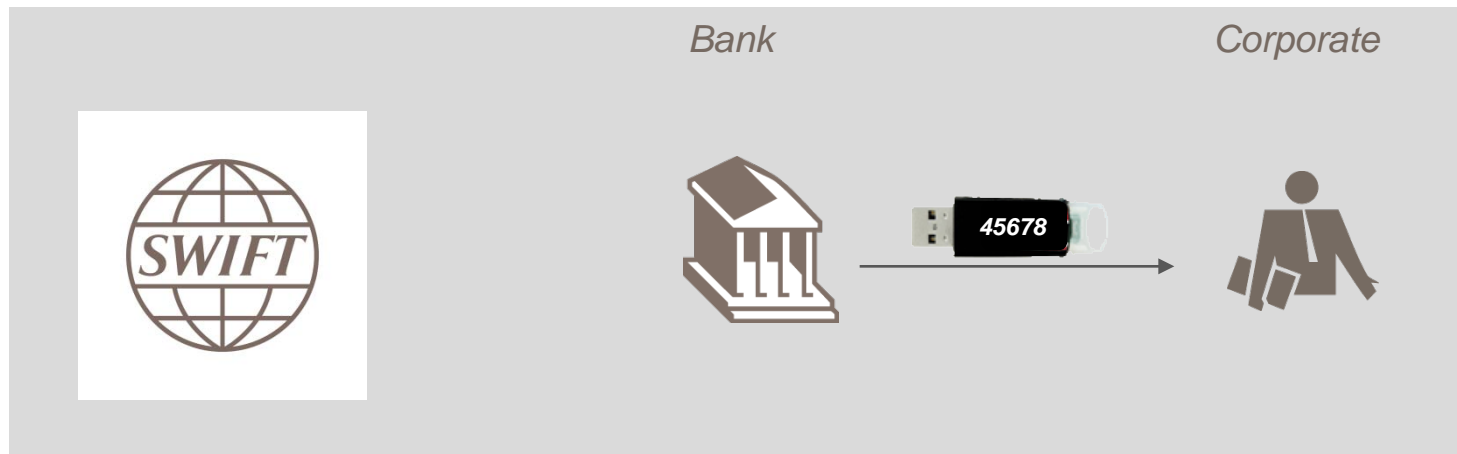
Corporate



- *USB token contains initial bootstrap data*
- *Security level is FIPS 140-2 level 2*

Overview of proposed solution

Step 2: Corporate receives an inactive token from a bank

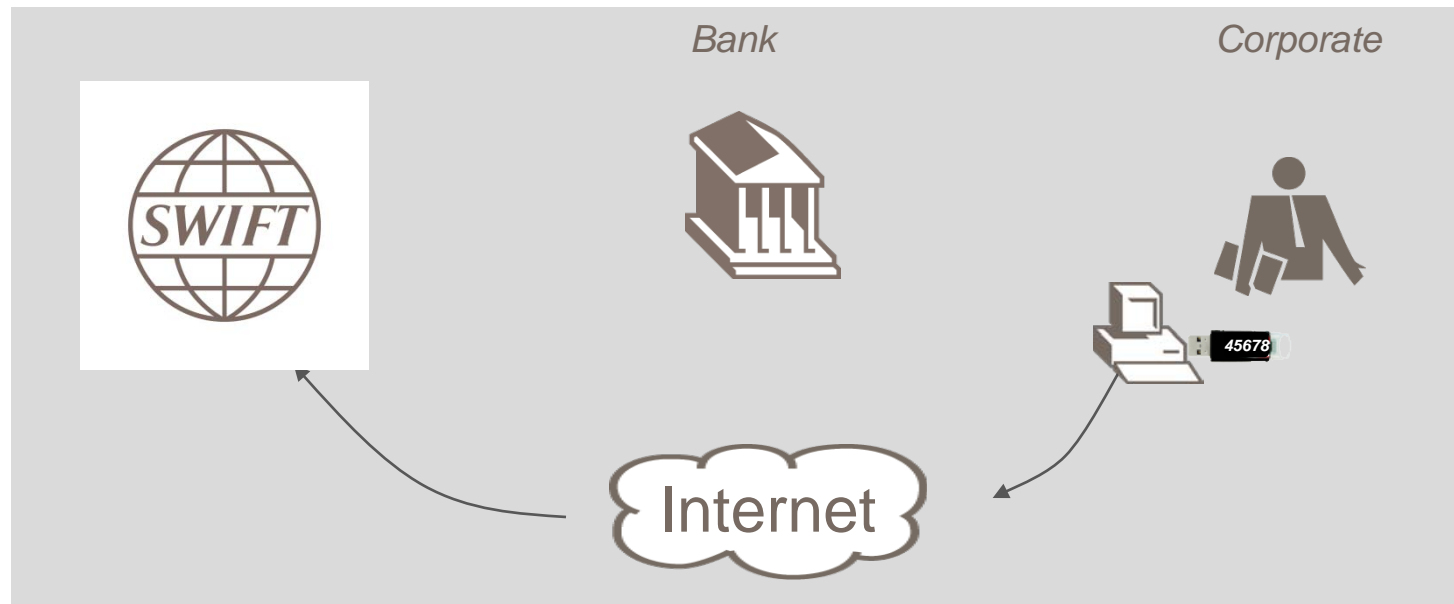


- *Tokens don't have critical value*
- *Certificate name is anonymous (eg o=swift, cn=45678)*

Overview of proposed solution

Step 3: Corporate user initialises the token

User activates the initial token by connecting to SWIFT

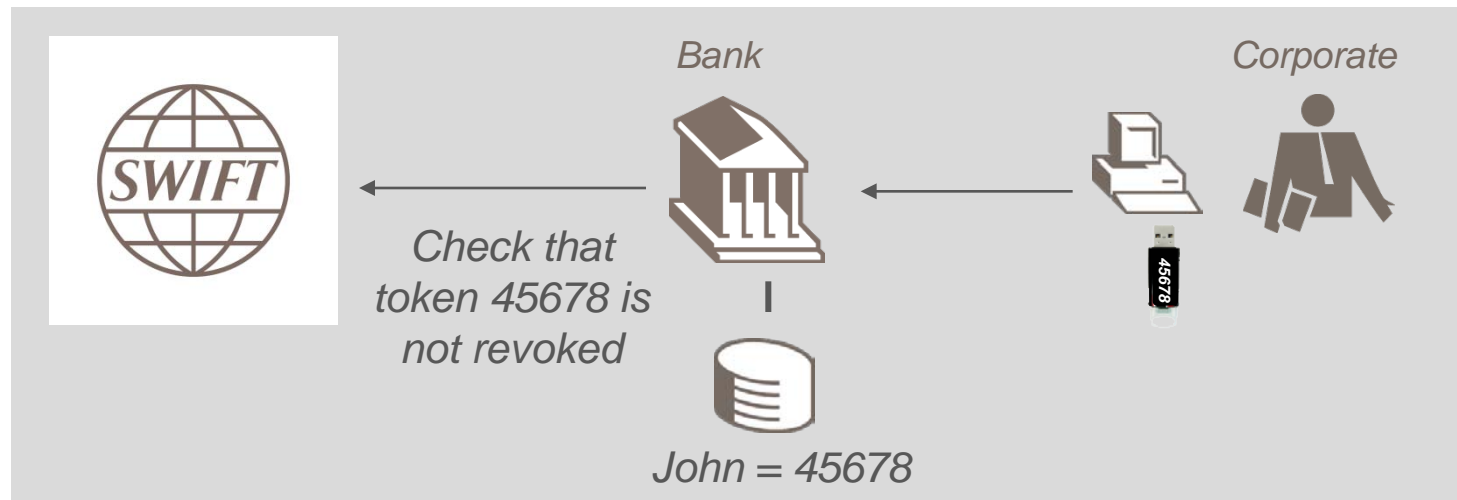


- *Generates a PKI key pair*
- *Certifies public key with SWIFT CA (accessible via Internet)*

Overview of proposed solution

Step 4: Corporate registers user with a bank

Bank maintains association between corporate user and activated token

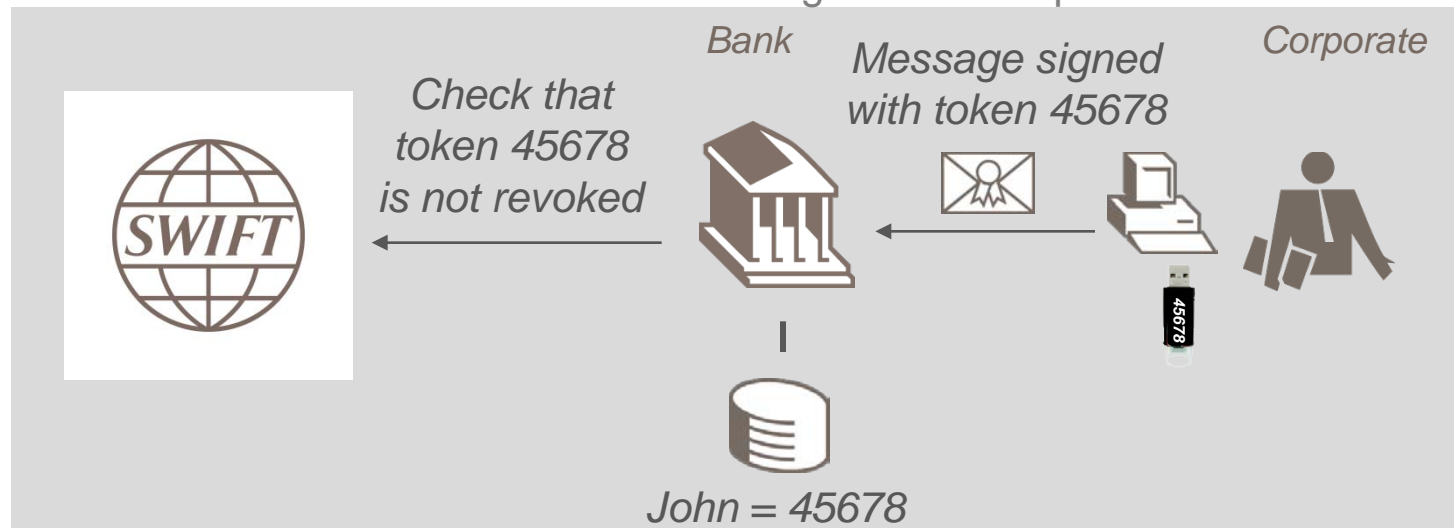


- *Value of activated token comes from registration with bank*
- *Bank must reliably identify token owner (physical presence or secure pre-existing remote identification technology)*
- *Owner signs with token to prove ownership*
- *Non-repudiable evidence of registration kept by bank*

Overview of proposed solution

Step 5: Corporate user uses the token for transactions

Transactions with the bank are signed with corporate user's token

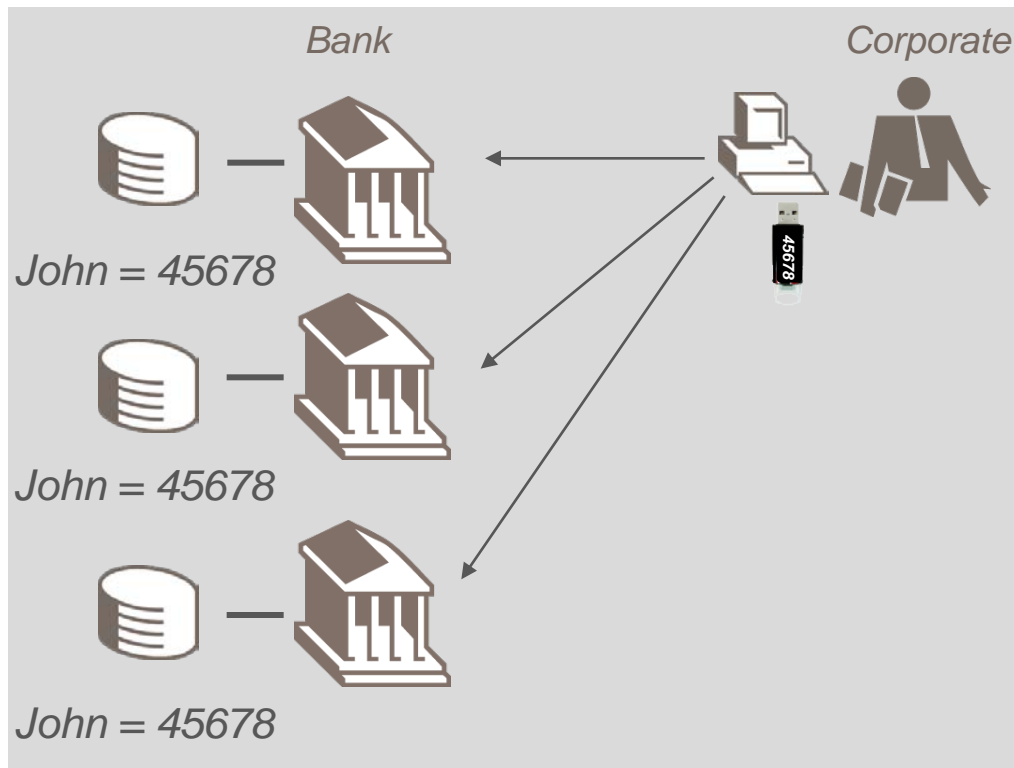


- *E-banking application signs messages with user's token (or ERP/TMS for SWIFTNet use)*
- *Bank's server software verifies signature*
- *Revocation check by downloading CRLs from SWIFT via Internet*
- *Signed message is non-repudiable evidence of transaction request*

Overview of proposed solution

Step 6: Corporate user applies same with other banks

Repeat step 4 (register with banks) and step 5 (send traffic) with other banks



- *John registers with other banks*
 - *To associate "John" with token "45678"*
- *Banks don't need to rely on each other for registration*
 - *But solution does not exclude such domestic arrangements*

Key benefits

For Corporates

- Convenience
- Lower cost
- Lower risk

For Banks

- Cost savings opportunity
- Better customer satisfaction

Status and next steps

- Project approved in June 2009
- Development, including definition of commercial offering has been initiated
- Pilot in Q1 2010
- Roll-out in Q2 2010
- Interoperability with other providers will also be provided



Thank you