

SWIFTNet Phase 2 Roadshow

This is a generic presentation.
Please make sure to add the
“country” specific information
on slides 20, 29 and 39.



Agenda

- **What is Phase 2 all about?**
- Customer impact overview
- Planning
- Where to find help?



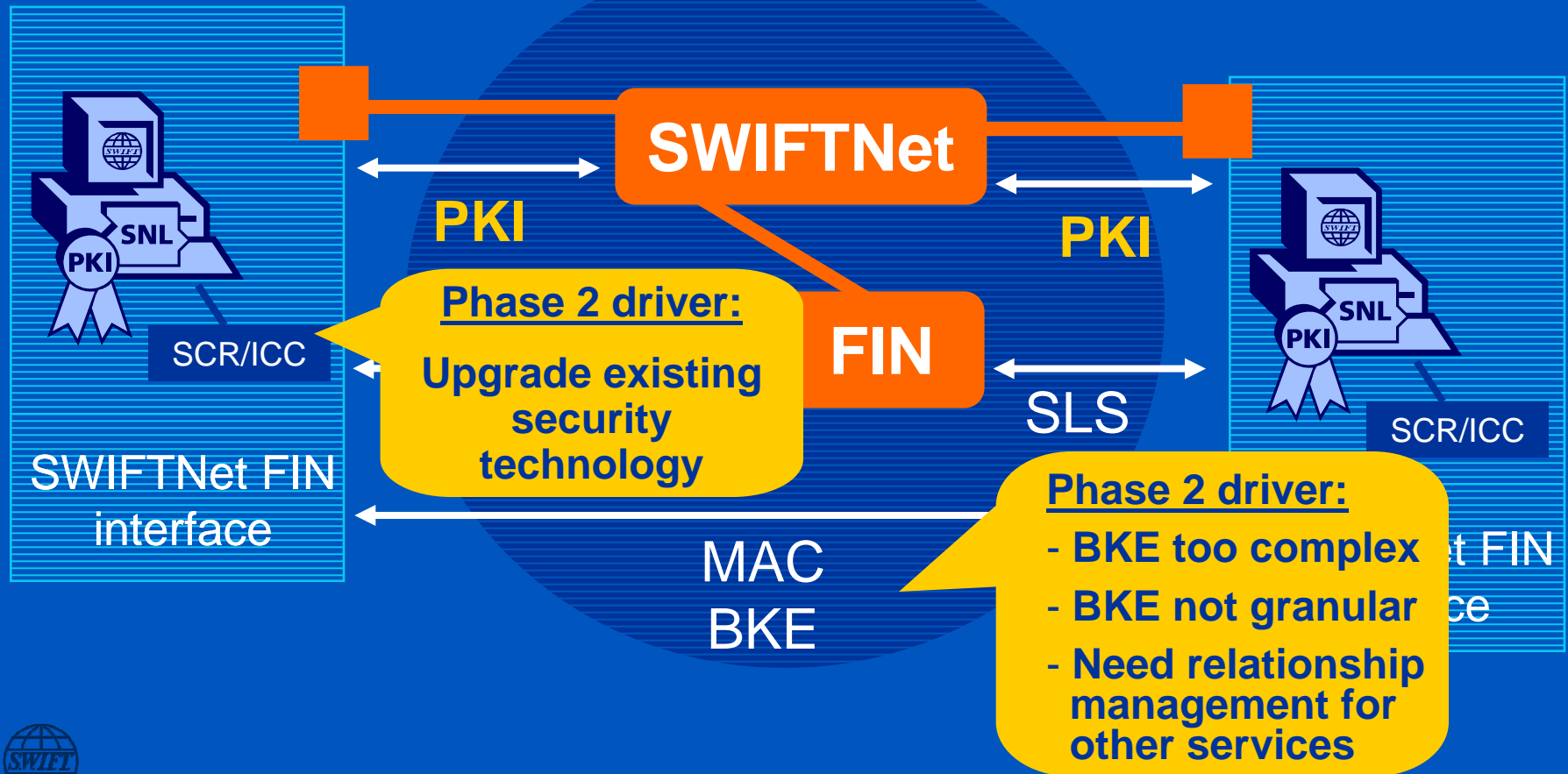
What is Phase 2 all about?

- **The basics**
- PKI
- HSM
- RMA



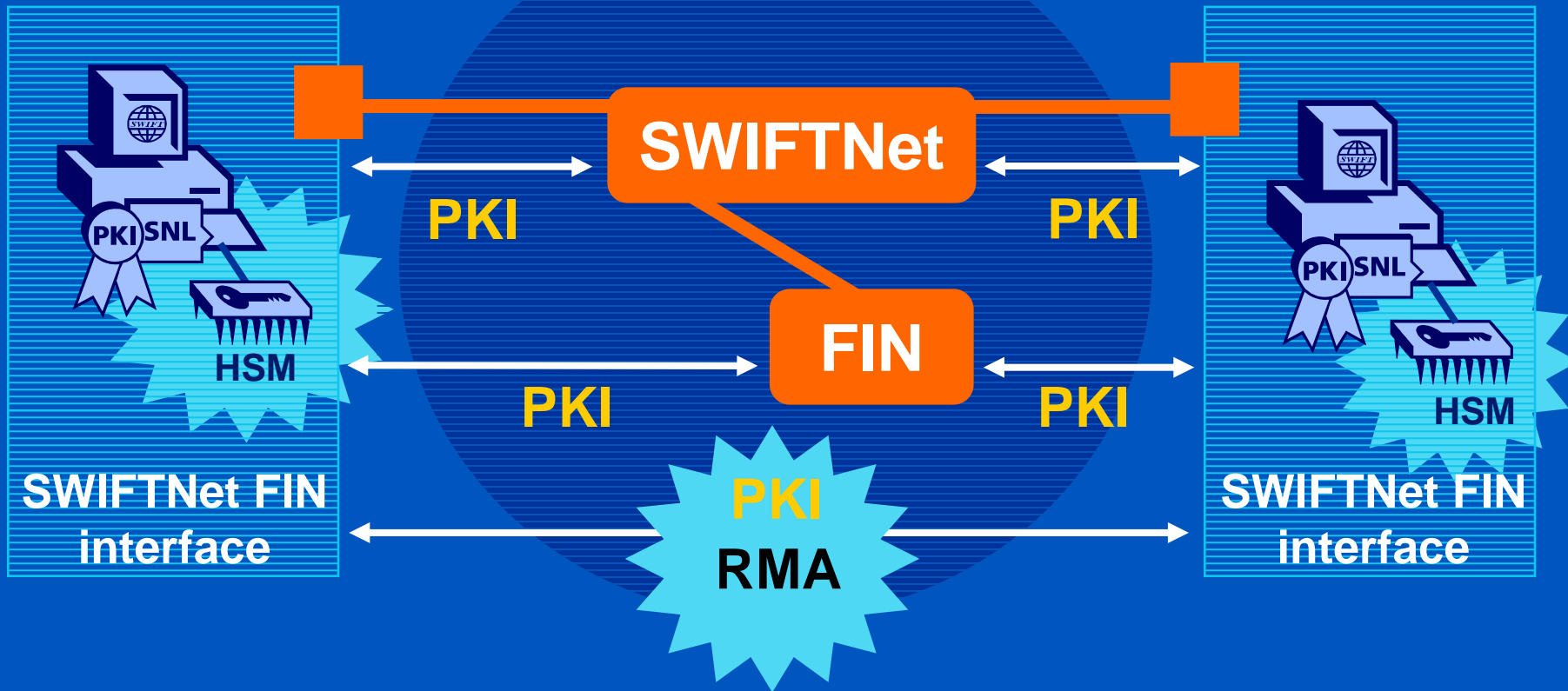
SWIFTNet FIN today

SLS: FIN Access control
MAC: End-2-end security
BKE: Relationship mgt.



SWIFTNet FIN Phase 2

PKI: FIN Access control
PKI: End-2-end security
RMA: Relationship mgt.

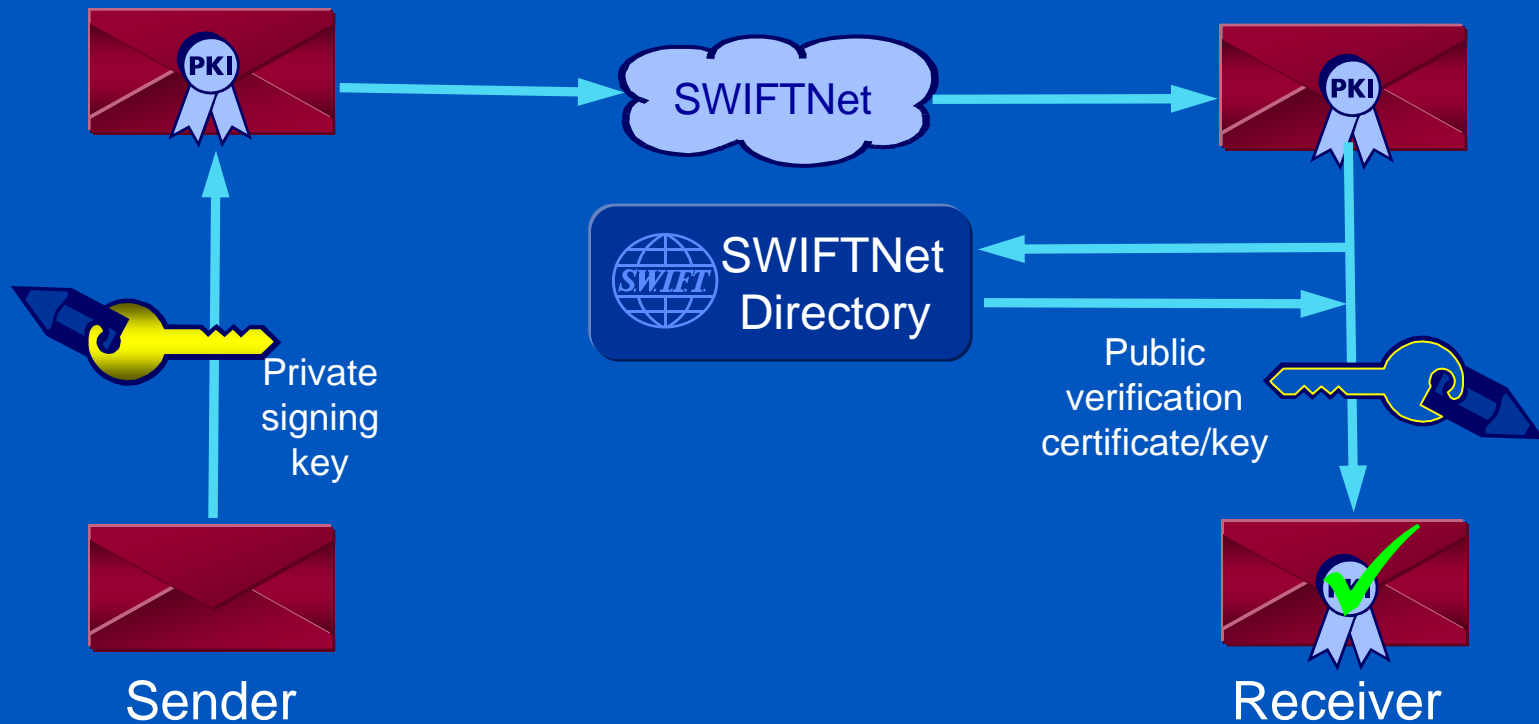


What is Phase 2 all about?

- The basics
- PKI
- HSM
- RMA



Introduction to SWIFTNet PKI

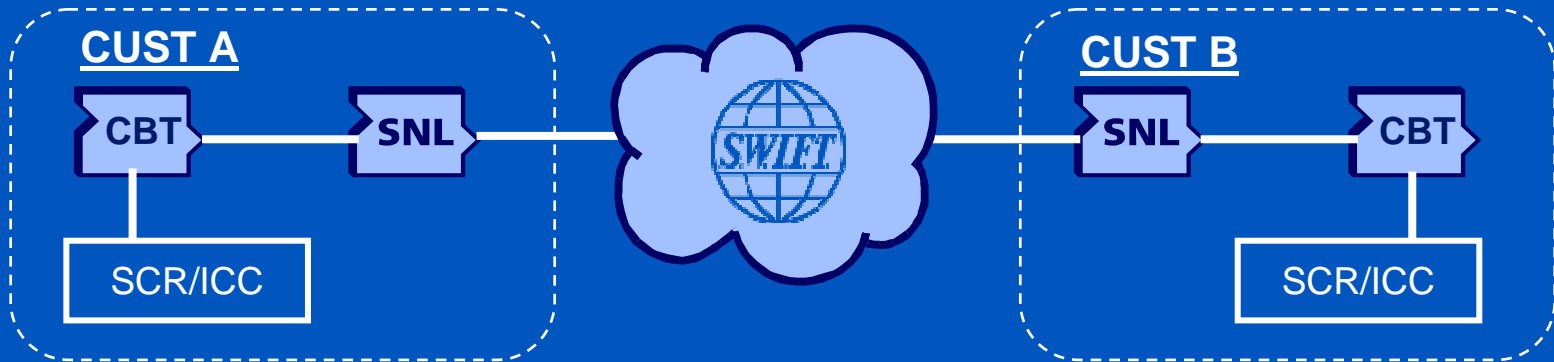


- Sender uses its private key to digitally sign the message
- Receiver uses the sender's public key/certificate to verify the digital signature. This guarantees integrity and authenticity



New SWIFTNet FIN security

FIN access control and user-to-user security



FIN access control security
~~S~~S (via ICC) → PKI

FIN user-to-user security
~~M~~C → PKI



PKI for SWIFTNet FIN

- LOGIN/SELECT secured by digital signature
- MAC/PAC are replaced with digital signature
- Sending BIC8 = Signing BIC8

{1:F01**AAAABBBCC**...}

... {5:~~MAC~~•~~AB~~1294F7}

PKI-signature from cn=fincbt1,o=**aaaabbbcc**,o=swift

MAC/PAC = 1 bilateral key per correspondent

PKI = 1 key (your own BIC8 key) for all correspondents

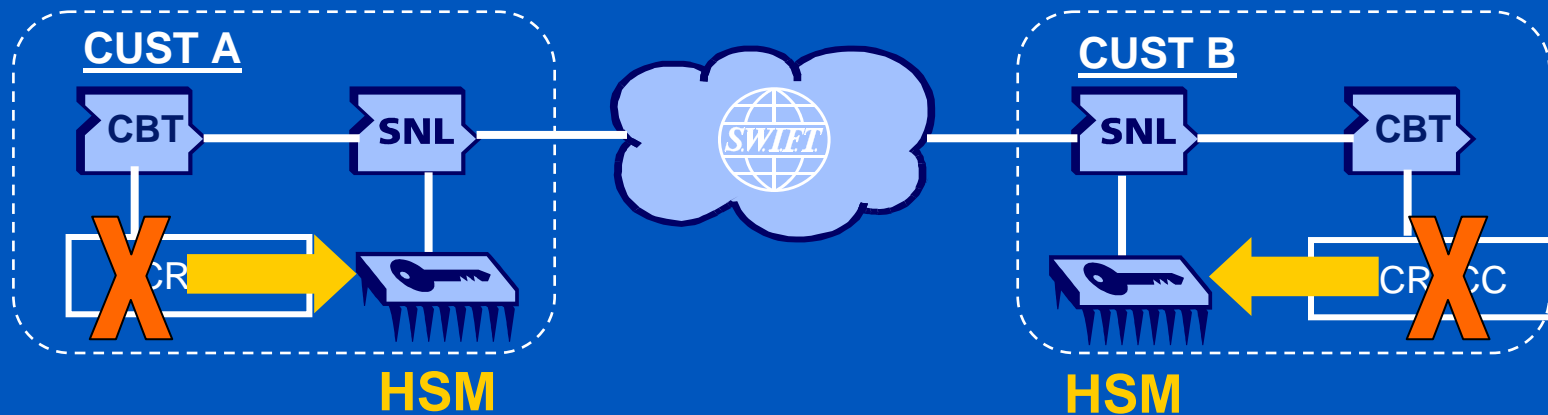


What is Phase 2 all about?

- The basics
- PKI
- **HSM**
- RMA



New security hardware



← FIN access control security →
PKI

← FIN user-to-user security →
PKI



Hardware Security Module (HSM)



- An **HSM** is a tamper-resistant hardware device used to securely store PKI private keys and to protect the generation of digital signatures

HSM protects:

- Generation & storage of private keys
- Generation of digital signatures



Hardware Security Module (HSM)

- Dedicated device for PKI signing operations
- Ordered at SWIFT

USB connected HSM

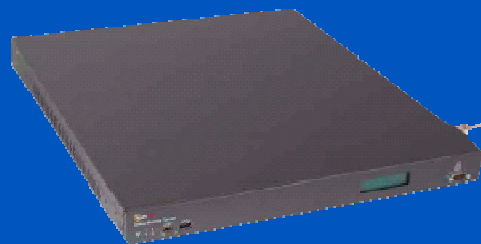
Windows SNL



500\$ (per set)

LAN connected HSM-box

Unix and Windows SNL



4,800 to 12,600\$ (per box)



HSM overview

HSM category	LAN connected HSM	USB connected HSM
Connectivity	LAN, can be shared between multiple SNLs	Directly inserted in USB port
SNL platform	Unix and Windows	Windows
Performance	<ul style="list-style-type: none">■ up to 3,600 msg/hour per low HSM box■ up to 18,000 msg/hour per medium HSM box■ up to 144,000 msg/hour per high HSM box	up to 1,000 messages per day per USB HSM
Storage capacity	Up to 250 certificates per box	1 certificate per USB HSM
Scalability	Up to 2 stand-alone boxes or 2 clusters per SNL	Up to 4 USB HSMs in parallel per SNL
Cluster support	Yes (2 boxes in cluster)	No



HSM pricing

- HSM prices include transportation and insurance costs, exclude customs duties and taxes

HSM pricing (USD)		
Item	One-Time fee	Annual maintenance
HSM box - high	12,600	2,520
HSM box - medium	9,000	1,800
HSM box - low	4,800	960
HSM tokens (8 pc)	500	(disposable item)
HSM cards (8 pc) & readers (4 pc)	500	(disposable item)



HSM Incentive

- SWIFT June board approval “2006 Pricing initiatives and commercial actions”
 - SWIFT is waiving the one-time fees of the HSM devices needed for SWIFTNet Phase 2
- Who?
 - For connection owners including Service Bureaus
- What?
 - USB HSM (tokens or card & readers):
 - For Windows users with 1 live BIC8 using connectivity pack 1 or 2
 - HSM Boxes
 - All other configurations
 - A pair of HSM boxes for prime connectivity pack + one HSM box for each additional connectivity pack



HSM Incentive ordering

- SWIFTNet Phase 2 Migration Kit
 - HSM + SWIFTNet release 6 software bundled
 - Order your Kit on www.swift.com before 15 December 2006



HSM Incentive shipment

- SWIFT will carry shipment, taxes and freight costs
- Standard maintenance charges for HSM Boxes start 3 months after shipment
- SWIFTNet Phase 2 Migration Kit shipped 3 months before your C1 Infrastructure Upgrade deadline



HSM resiliency



- No live FIN authenticated messages can be sent without HSM

HSM resiliency!

- **For USB connected HSM**

- Backup tokens or cards/readers included in the initial package
- Replacement package can be ordered

- **For LAN connected HSM**

- Mandatory second box (cluster recommended)
- Additional spare box recommended for critical systems (avoid Single Point of Failure during box replacement)
- Advanced box replacement



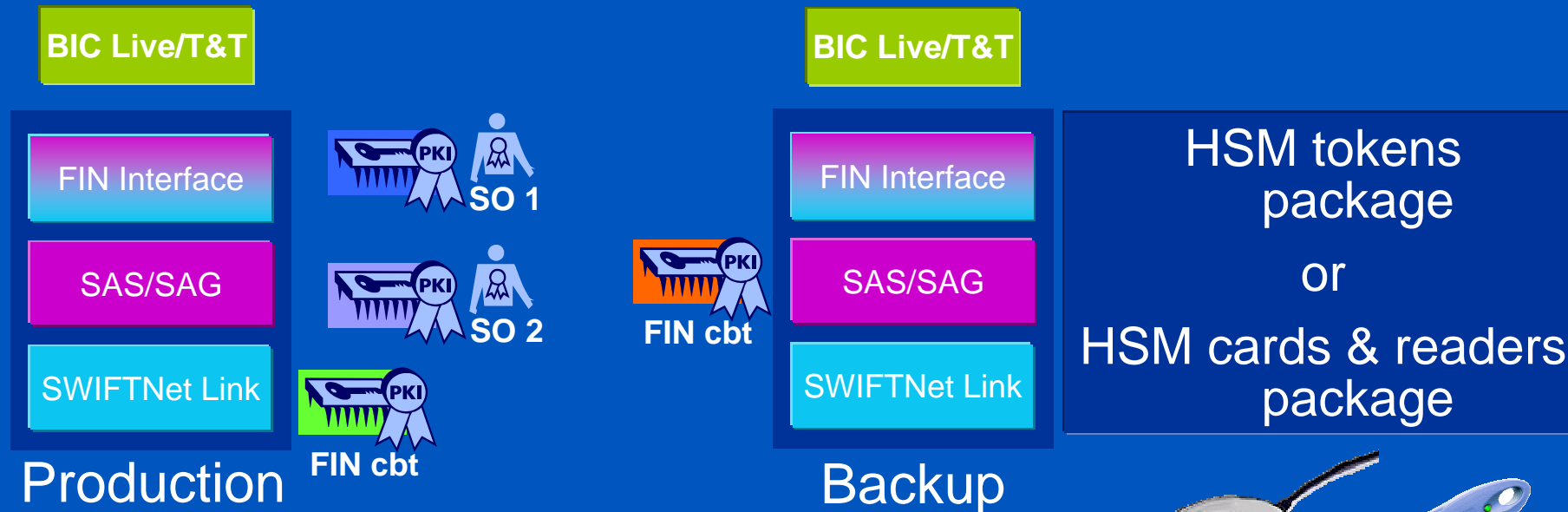
“Country”

Specific HSM importation information

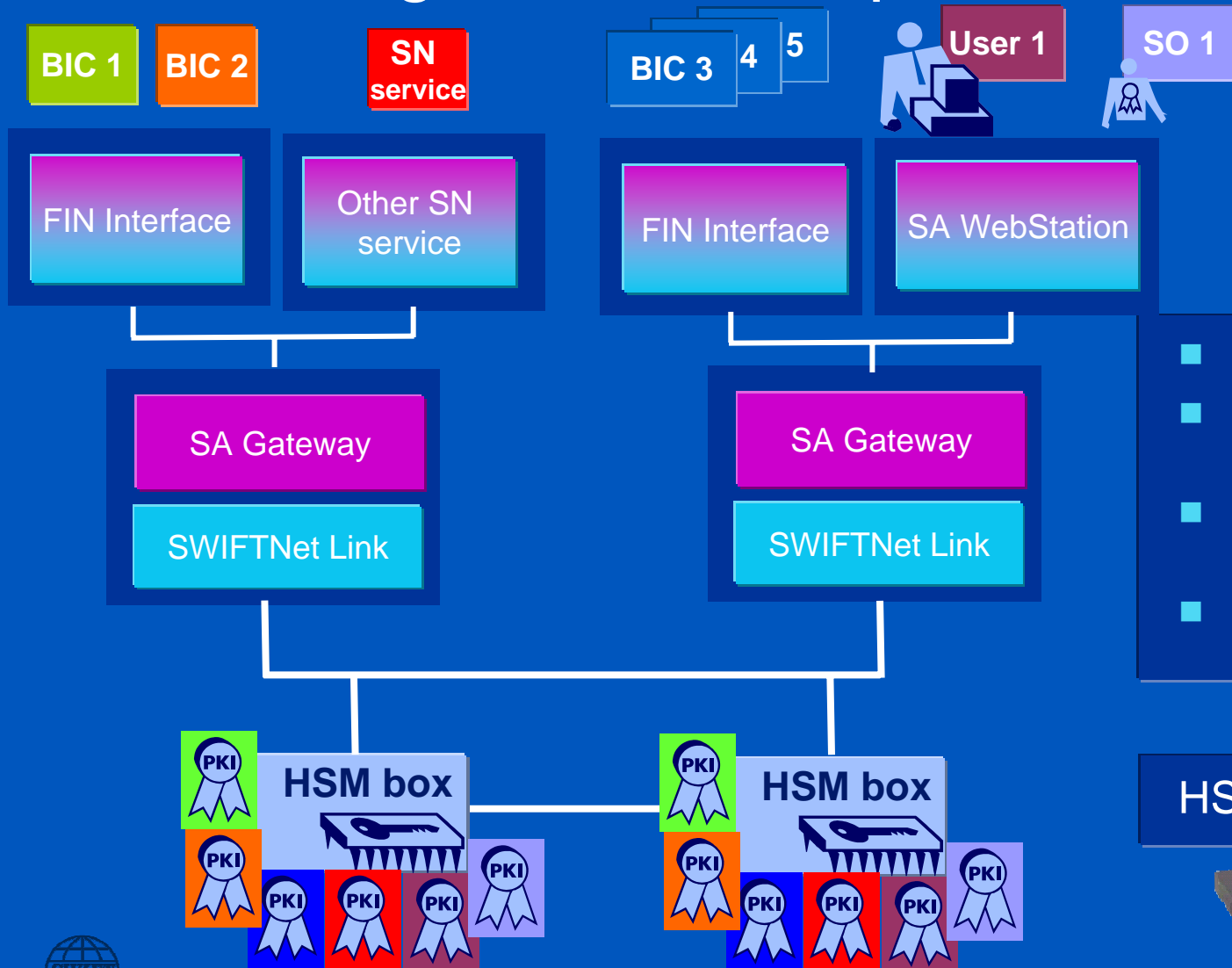


HSM configuration examples

- 2 Security Officers (SO), one FIN certificate per BIC
- Maximum 1000 FIN messages per day per USB HSM per BIC
- 4 USB HSM are supported per SNL on Windows
 - If 4 USB ports available on the SNL PC

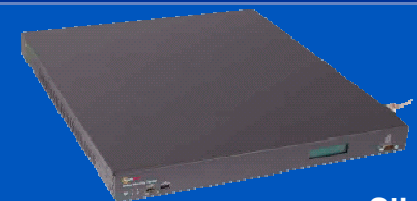


HSM configuration examples



- Multi FIN BICs
- Multi SWIFTNet services
- Over 1000 FIN messages per day
- SNL on AIX or Solaris

HSM boxes in cluster

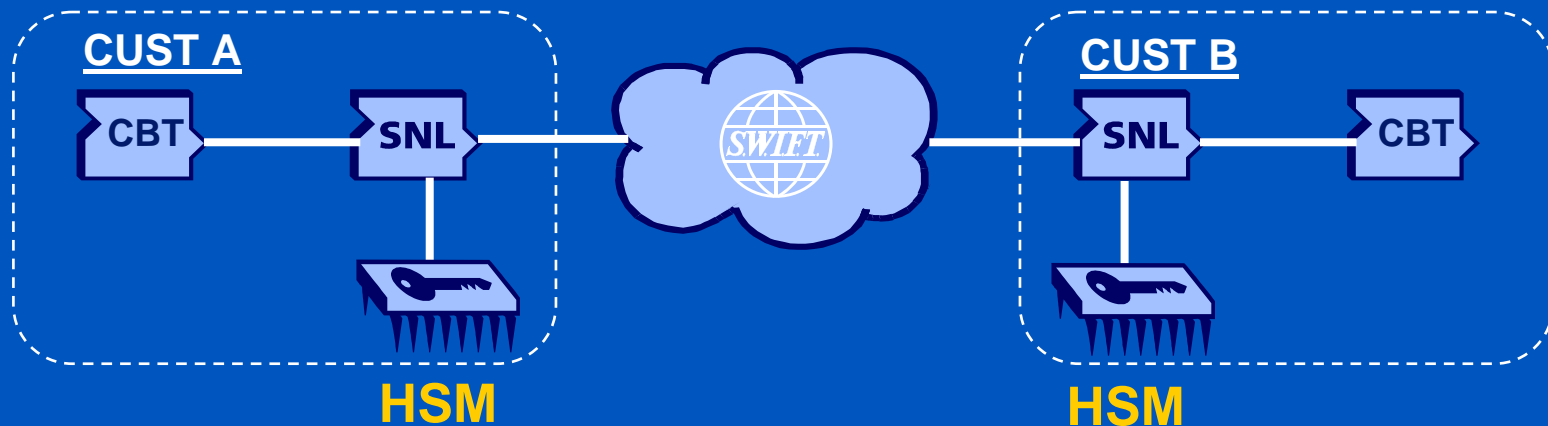


What is Phase 2 all about?

- The basics
- PKI
- HSM
- **RMA**



In 2008 new relationship management



FIN access control security
PKI

FIN user-to-user security
PKI

Relationship management
BXE → **RMA**



Relationship management application (RMA)

- Managing correspondents in a many-to-many world
 - RMA as mechanism to control WHO can send you traffic
- Managing the correspondent's business
 - RMA as mechanism to control WHAT a correspondent can send to you

Objective: preventing unwanted traffic

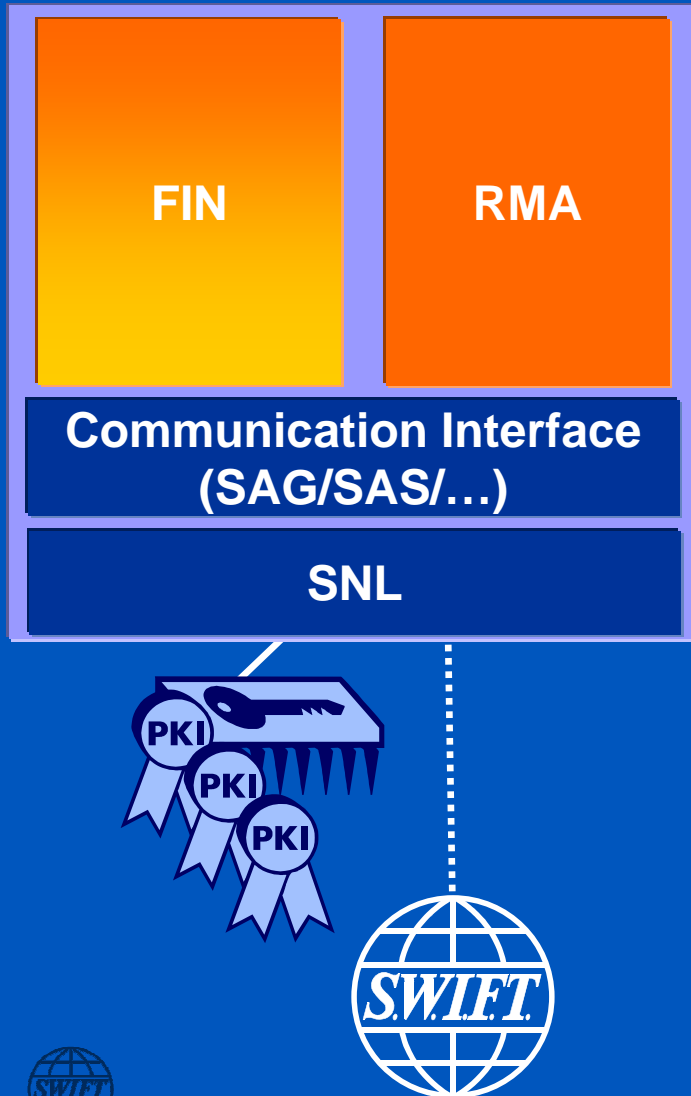


Agenda

- What is Phase 2 all about?
- **Customer Impact overview**
- Planning
- Where to find help?



SWIFTNet FIN Phase 2 : customer impact overview



What's required:

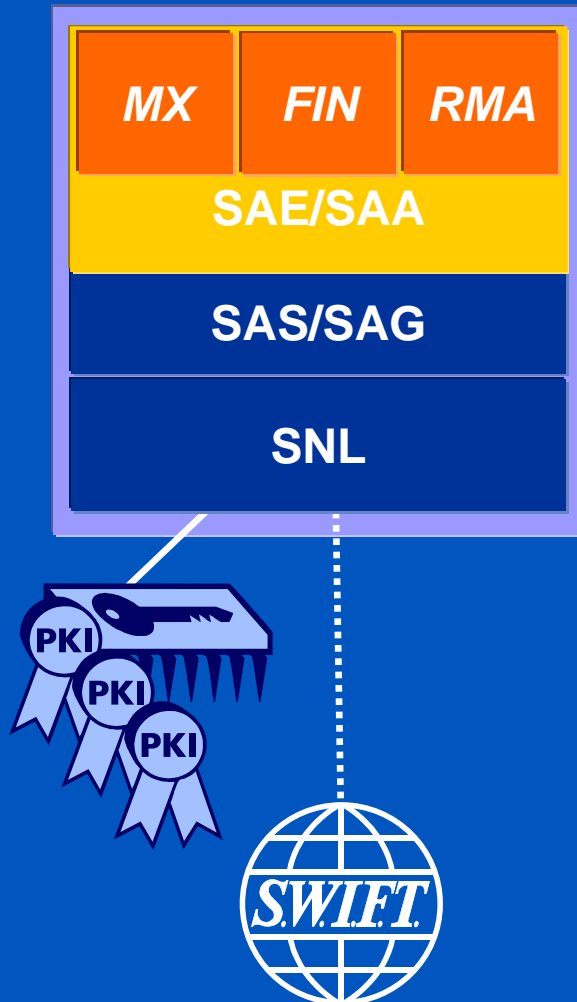
- R6 SNL/SAG... upgrade
- FIN Interface upgrade
- HSM's
- Certificates + Security Officers (if not existing)
- RMA interface

Check impact on Back-office:

- Aware of MAC/PAC?



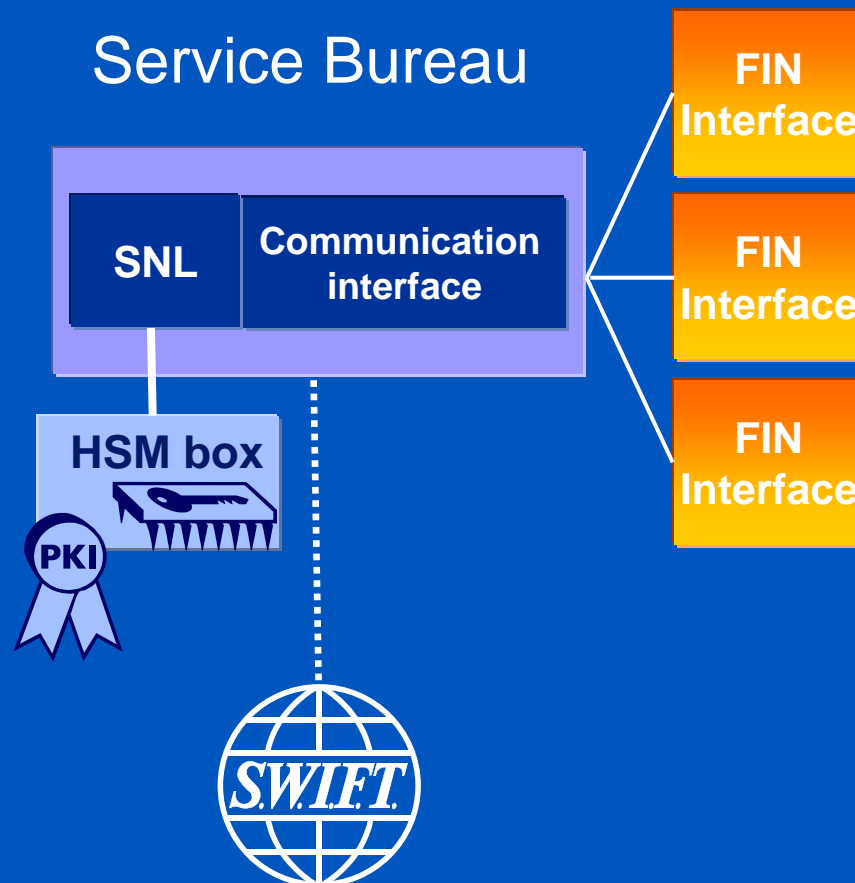
SWIFTNet FIN Phase 2 for a SWIFTAlliance user



- SAA/SAE R6 upgrade for the FIN changes
 - PKI
 - HSM support
 - RMA functionality
- SAS (Starter Set) or SAG needed



SWIFTNet FIN Phase 2 for a Service Bureau user



- R6 upgrade required
- HSM connected to SNL
- Service Bureau orders and installs the HSM



What will change in daily operational procedure

■ (current) ICC for LOGIN/SELECT



ICC cards with pin codes
for the 3 operators

■ (new) PKI/HSM for LOGIN/SELECT



PKI and HSM used for:

- Login/Select
- Signing FIN MT

HSM connected to SNL machine !

3 operators with Login/Select permissions



**Defined in
permissions/profile
of operators on SAA**



Agenda

- What is Phase 2 all about?
- Customer Impact overview
- **Planning**
- Where to find help?



Planning

- **Phase 2 migration principles**
- Timelines and milestones



Principles

■ No big bang

- Migrate BIC8 by BIC8
- Migrate independently of correspondents and of central institution
- Fall back capability available
- Co-existence of Phase 1 security and Phase 2 security

■ Spread workload to maintain quality

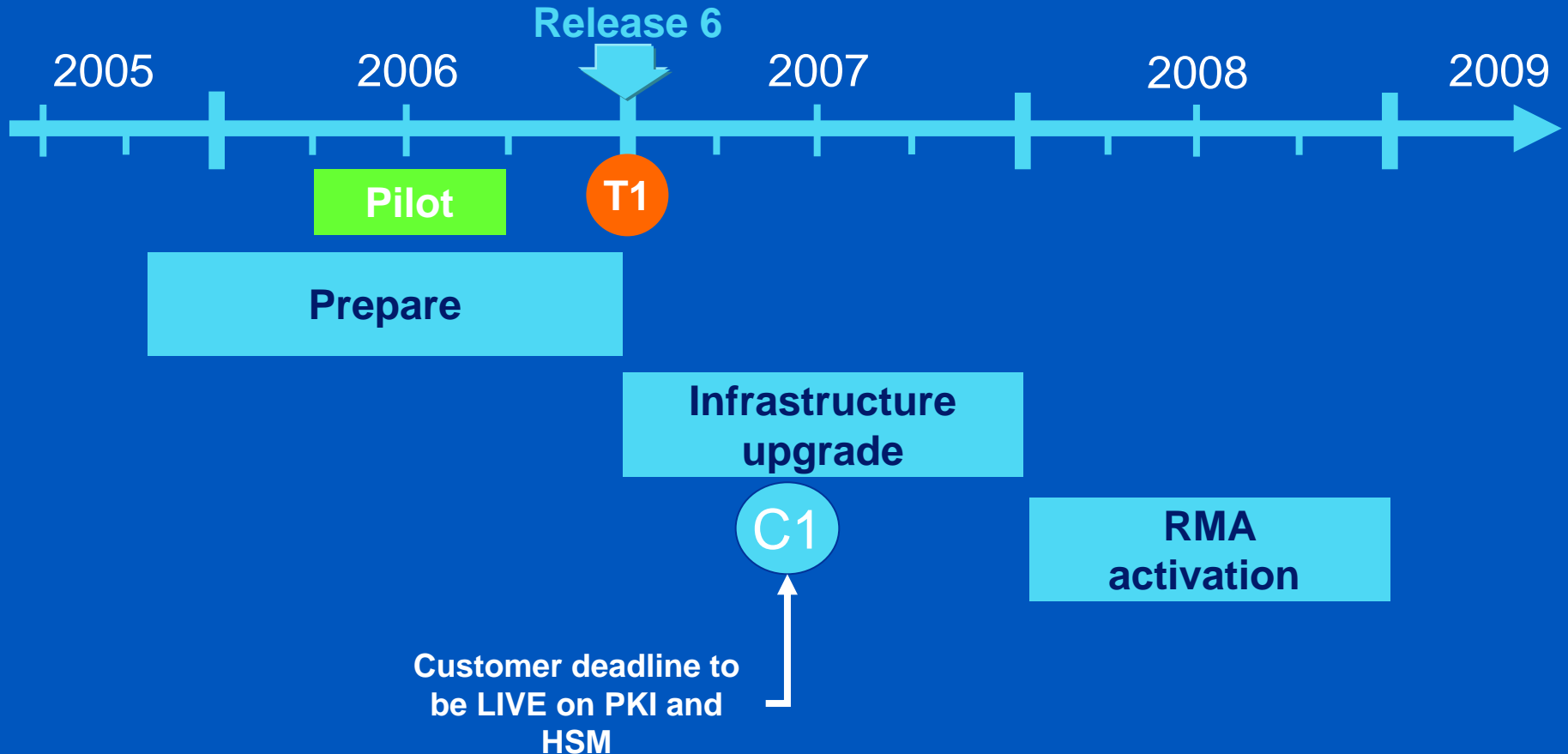


Planning

- Phase 2 migration principles
- **Timelines and milestones**



SWIFTNet Phase 2 timeline



Prepare now !



■ PKI and Security Officers

- If your live BIC8 doesn't have own PKI & Security Officers yet, you can sign up for it now
 - Shared Security Officers recommended

■ HSM information via www.swift.com

- Make sure you have access!
- On-line configurator to assist in HSM selection

■ Prepare your OS upgrade now (needed for SWIFTNet release 6)

- Windows 2003 (Windows XP for SAB)
- Solaris 10
- AIX 5.3
- For more details, check the latest SWIFTNet Interfaces release overview (Knowledge Base tip 639899)



Prepare now !



- **For SAA/SAE users, install SWIFTAlliance Starter Set if not yet done**
 - SWIFTAlliance Starter Set waiver campaign finished
 - If not yet used, your voucher will expire end December 2006 !
 - SAS campaign voucher can be used for:
 - Free education courses
 - eligible SWIFT Training courses list included in voucher communication
 - see swift.com for the Training Calendar in your region
- OR
- Free Service Partner installation assistance
 - Contact a Service Partner to agree on a date for the on-site visit



www.swift.com/swiftnetphase2

Ordering portal and Configurator portal

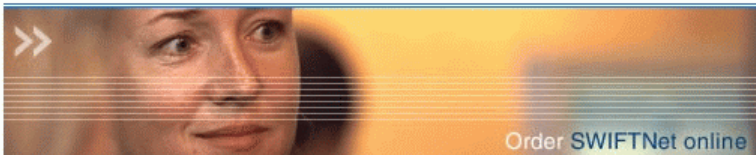


SWIFT.COM – THE PRIME NEWS AND
INFORMATION CHANNEL FOR THE SWIFT COMMUNITY

My profile BIC directory

Home About SWIFT Products & Services Support Partners Standards

Support > Ordering



Ordering

Updated 21 November 2005

SWIFT Ordering enables you to order products, services, training and documentation as well as upgrading, changing and terminating existing installations.

This ordering page covers most standard configuration options, but is not intended to handle more complex set-ups. For such cases, we encourage you to contact your local [SWIFT office](#) before placing an order. If you have any questions about the ordering page or SWIFTNet ordering in general, please refer to the [Knowledge base](#).

Order our products & services

SWIFT MEMBERSHIP

New	Change	Terminate
» Become a SWIFT User	» Changing SWIFT User category	» Resign from SWIFT
» Request additional BIC/BEI		» Deactivate connected BIC/BEI

SECURITY

Register	Change	Terminate
» Main SWIFTNet Security Officers	» SWIFTNet Security Officer Registration	» Additional SWIFTNet Security Officer
» Main SWIFTNet Security Officers of Service Bureau	» SWIFTNet FIN Security Officer Information	
» Shared SWIFTNet Security Officers		
» Additional SWIFTNet Security Officers		
» SWIFTNet FIN Security Equipment		
» SWIFTNet FIN Security Officer		



SWIFT.COM – THE PRIME NEWS AND
INFORMATION CHANNEL FOR THE SWIFT COMMUNITY

My profile BIC directory Search... Search

Home About SWIFT Products & Services Support Partners Standards Training Conferences

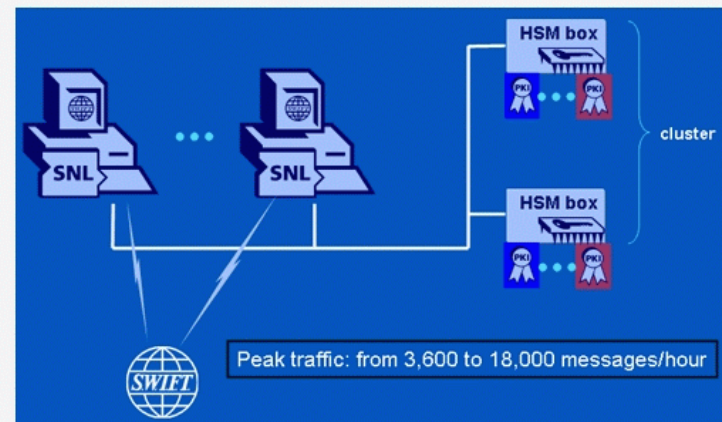
Log out

Selected configuration

Which business services do you use on SWIFTNet?	Fin only
How many FIN BICs does this site host?	One BIC
Daily average of live FIN traffic (input & output)	15000
FIN traffic yearly growth rate	10 %
Computed peak traffic per hour	5500

Two Medium HSM boxes

The advised HSM configuration is medium HSM boxes (from SafeNet) set-up in a cluster. A HSM box can store up to 250 security profiles. An SNL supports up to 2 stand-alone HSM boxes or 2 clusters. For resilience purposes, at least two boxes must be ordered. Additional spare boxes can be ordered.



◀ Back

▲ reset

Customer scheduling

■ Milestone C1

- Allocation based on location of SWIFTNet connection
- Completion of the infrastructure upgrade
 - SNL, SAG, SAB Release 6
 - FIN interface upgraded
 - HSM installed with PKI secrets

■ ‘Your country’ C1 deadline is ‘.....’

- You are using PKI and HSM for your live (and test) SWIFTNet FIN traffic
- All installation, testing and live ramp-up activities are completed



Surcharges and penalties

- **After your C1 deadline**, if you are still using Login/Select via ICC you will have to pay a surcharge of **1000 EUR per month per BIC8**
- If you are still using Login/Select via ICC by January 2008 you will pay the following penalty per BIC8:
 - January 2008: **5000 EUR** per BIC8
 - February 2008: **10000 EUR** per BIC8
 - March 2008: **20000 EUR** per BIC8



Wallchart

SWIFTNet FIN Phase 2 Plan

Timeline:



2006
Prepare

For detailed instructions on how to complete each stage, see the SWIFTNet FIN Phase 2 Migration Guide. The migration steps that appear in grey are not applicable to all participants.

Preparing to Upgrade

Awareness

- ☐ Register for the SWIFTNet FIN Phase 2 roadshow.
- ☐ Attend the roadshow.

Visit the SWIFTNet FIN Phase 2 section of www.swift.com to do the following:

- ☐ Read the SWIFTNet FIN Phase 2 documentation.
- ☐ Check availability of training courses.

Budgeting

- ☐ Use the configurator tool on www.swift.com
- ☐ Contact your interface supplier.
- ☐ Contact your local Service Partner.

Planning

- ☐ Check your migration schedule on www.swift.com
- ☐ Enter your dates on the timeline at the top of the chart.
- ☐ Create a migration project team.
- ☐ Register for training courses.
- ☐ Analyse your ordering needs. Check that you have the following:
 - registered shared Security Officers for each BIC8
 - interfaces and licences for all BIC8s
 - operating system upgrades
 - appropriate hardware
 - RMA software
 - HSM type



Wallchart (2)

anner

T1

C1 - 9 weeks


/ / ← Ordering period → / /

General availability

Ordering deadline

the relevant section in the SWIFTNet FIN Phase 2 Planning Guide, customers.

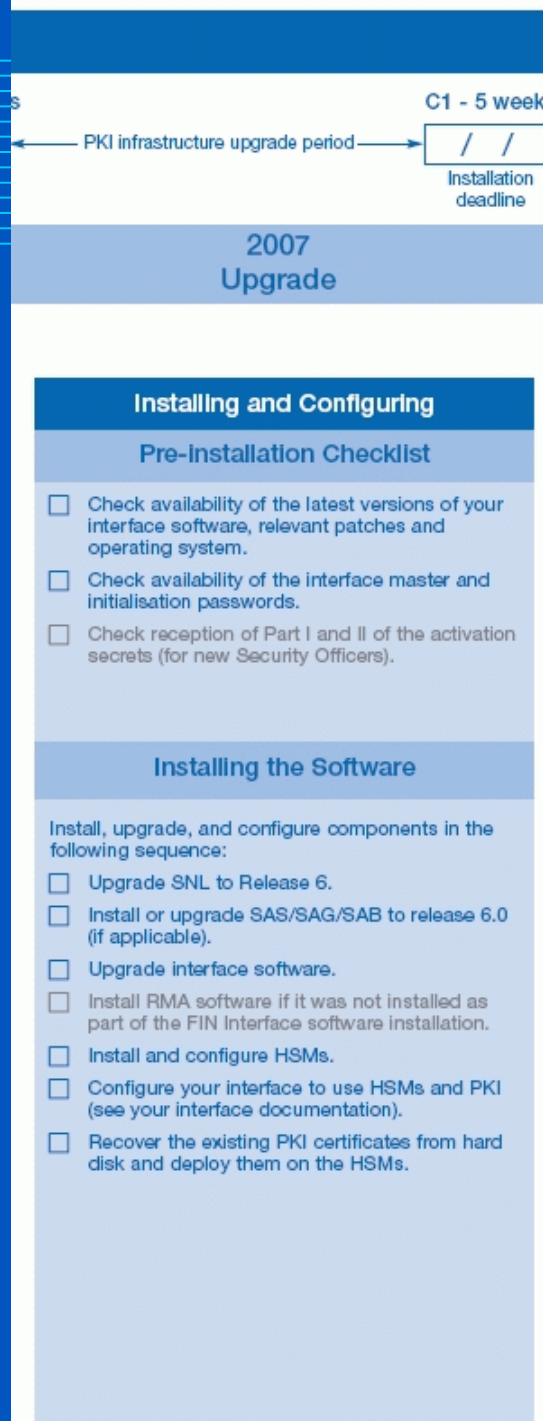
Ordering

 You must complete all orders nine weeks before your C1 date (depending on your country, allow more time for import and customs delays).

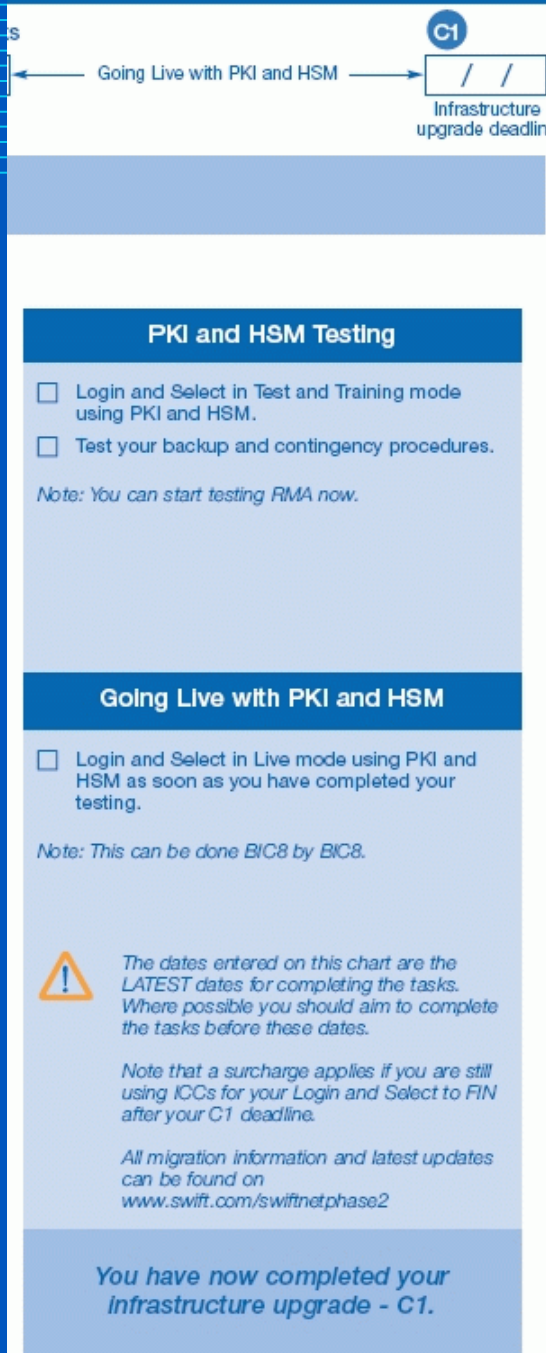
- ☐ Submit your HSM order to SWIFT.
- ☐ Order RMA software (if you are not a SWIFTAlliance user).
- ☐ Register Security Officers (SOs) for all of your live BIC8s if not yet done. Note that you can choose between your own and Shared Security Officers (SSOs).



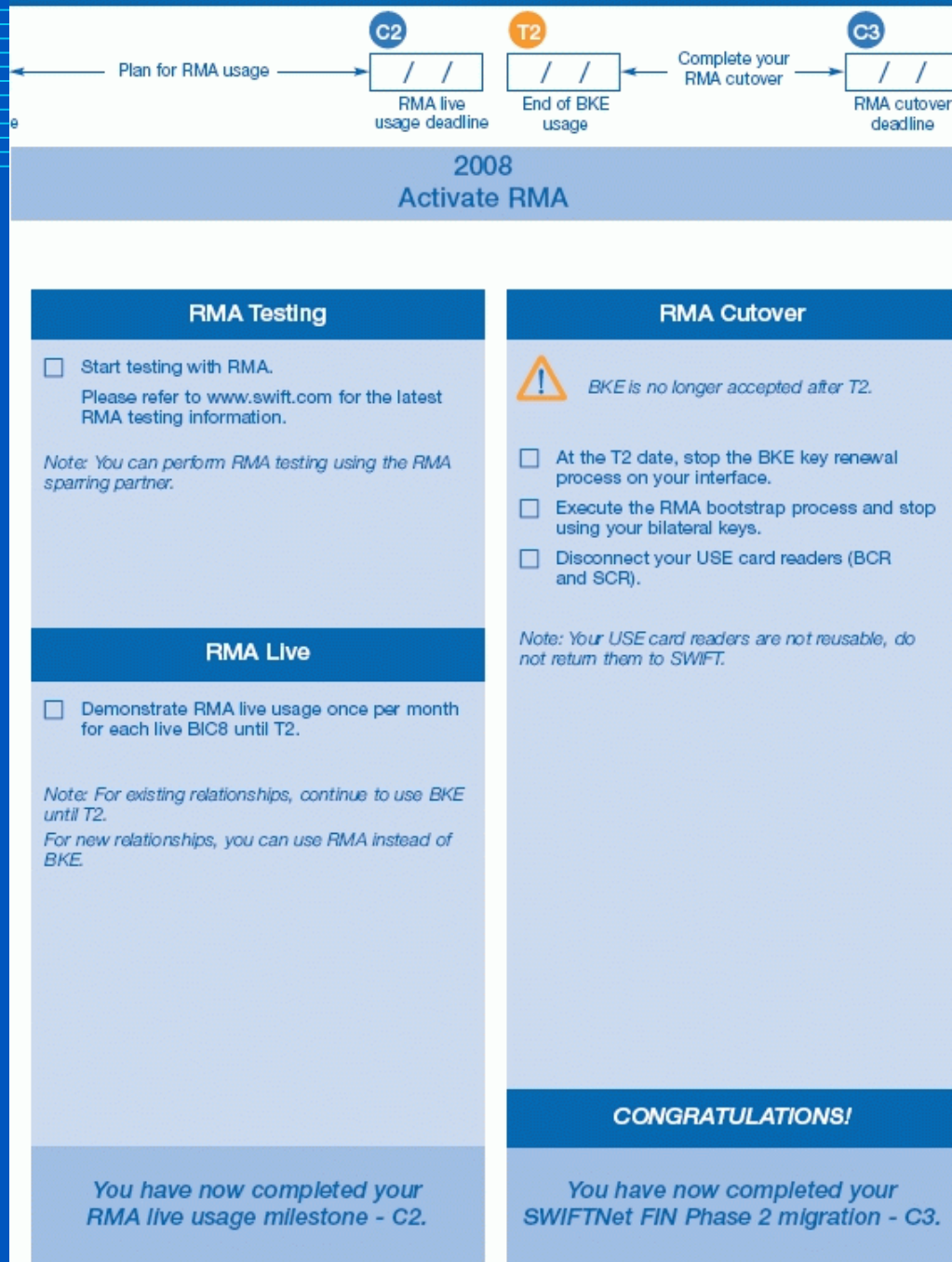
Wallchart (3)



Wallchart (4)



Wallchart (5)



Agenda

- What is Phase 2 all about?
- Customer Impact overview
- Planning
- **Where to find help?**



Where to find information



- www.swift.com/swiftnetphase2
 - Information paper, Overview document, FAQ
 - Planning guide and Wallchart planner
 - HSM on-line configurator
 - Download the generic roadshow presentation
- www.swift.com/support
 - Knowledge Base
- Consult your interface vendor



Register now with SWIFTSupport



- Register **ASAP** to SWIFTSupport online service at www.swift.com/support
 - Click on Register and select “Register for SWIFTSupport” and follow the steps
 - You will then receive:
 - your **password** to use SWIFTSupport online services
 - your **personal registration card**
- As of July 2006, non registered customer will no longer be entitled to our support services
 - At least 2 people per location should be registered by July 1st, 2006

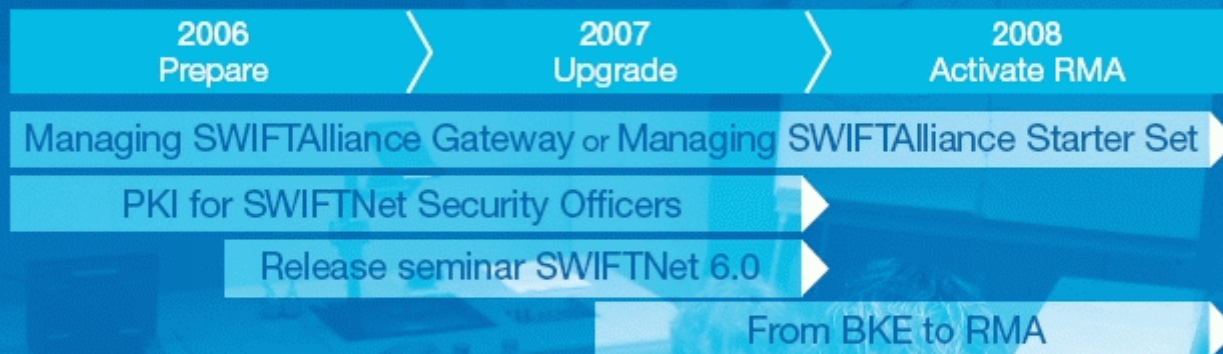


You want to know more...

■ Attend one of our SWIFT trainings

Migrate smoothly with SWIFT Training

SWIFTNet Phase 2 courses



For more information on SWIFT Training, please visit www.swift.com/training.



You want to know more...

- **Check regularly our training website** at <http://www.swift.com/training> for future coming trainings:
 - Release seminar SWIFTNet 6.0, From BKE to RMA, ...
- **Contact your FIN Interface vendor**
- **Contact your Service Partner**



Summary...

- **Plan & budget to meet your Infrastructure Upgrade deadline in 2007 !**
- Prepare now
 - Use the HSM online configurator
 - Check PKI & Security Officer registration
 - Plan your OS upgrade
 - For SAA/SAE users: install SWIFTAlliance Starter Set if not yet done



SWIFTNet FIN Phase 2

It's time to prepare !



A woman with glasses and a turtleneck sweater is speaking into a microphone. The image is overlaid with a blue gradient and horizontal lines.

Questions & answers

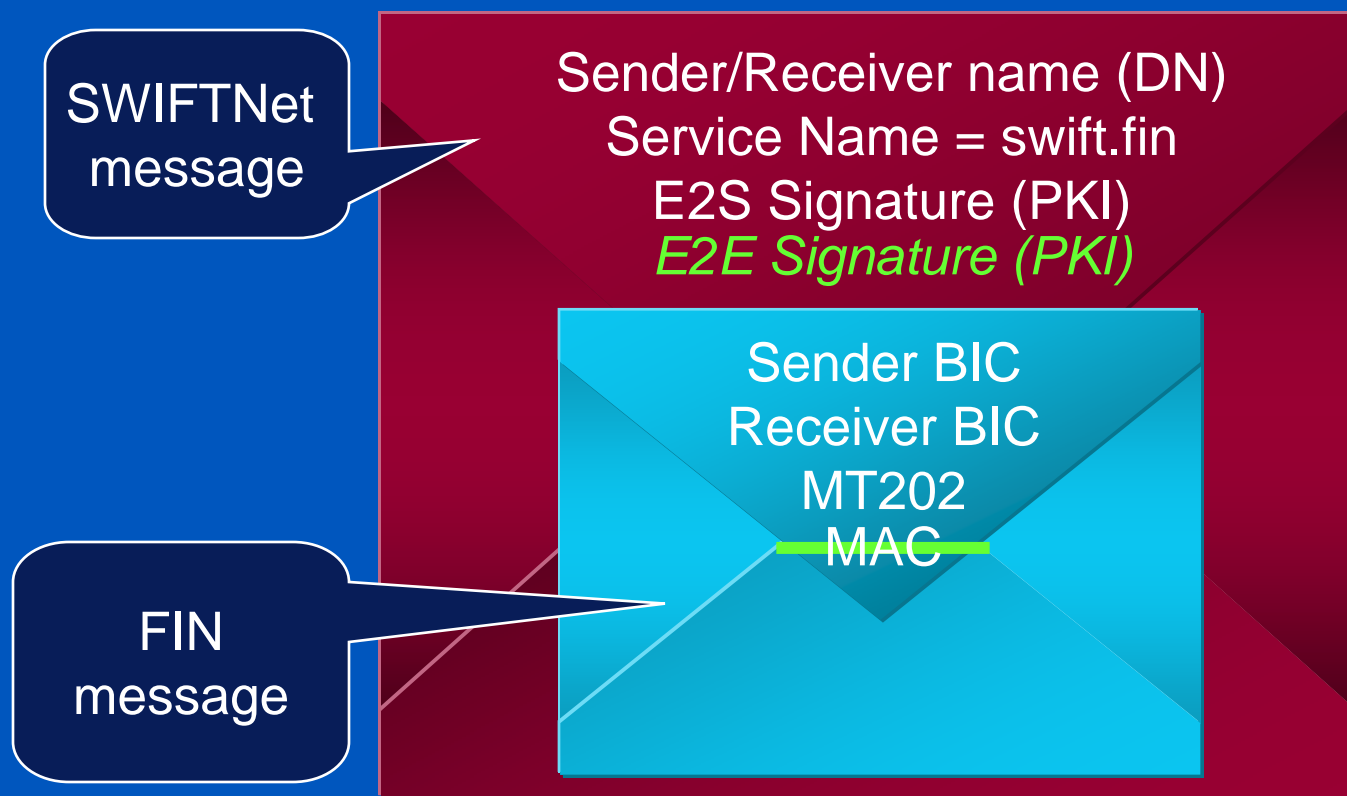


Back-up slides

- SWIFTNet FIN Phase 2 message
- HSM scope
- RMA



SWIFTNet FIN Phase 2 Message



HSM scope: mandatory usage

For SWIFTNet FIN Phase 2

- **FIN Live messages**

must be signed using an HSM

- technically enforced

- **FIN Test & Training messages**

recommended to use HSM

- to simulate the production environment
e.g. throughput tests



Relationship management application (RMA)

■ Managing correspondents in a many-to-many world

- RMA as mechanism to control WHO can send you traffic
- Preventing ‘unwanted traffic’

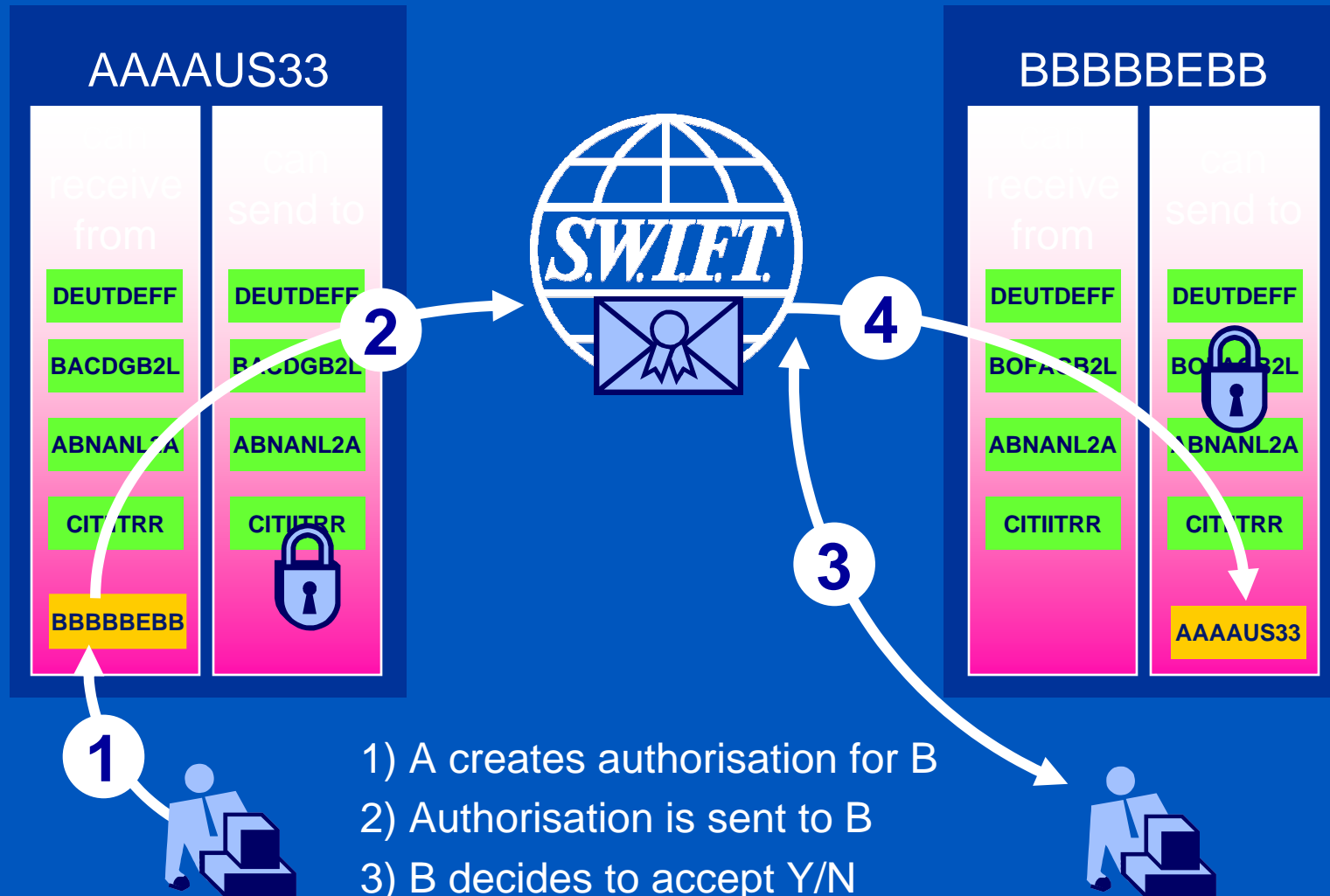
■ Managing the correspondent's business

- RMA as mechanism to control WHAT a correspondent can send to you
- Example, for FIN:
 - Authorisations only apply to authenticated traffic
 - Authorisations can be granular to the level of MT/MT category



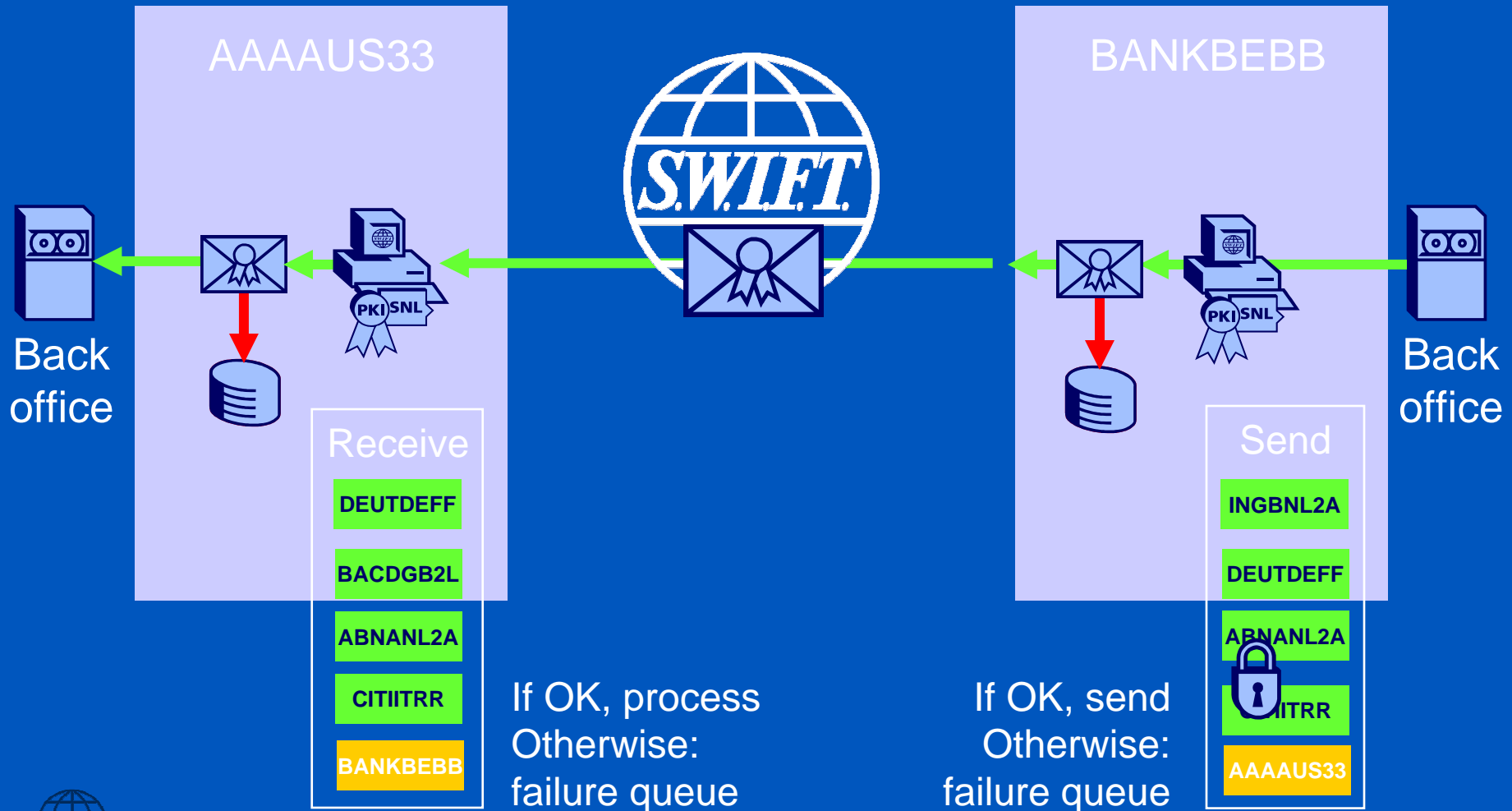
RMA interface

RMA - Correspondents exchanging authorisations



FIN interface

message filtering - B sends message to A



RMA future proofing

- **RMA service is designed for all SWIFTNet services**
 - to control counterparts and traffic
 - define what will be allowed (in/out) per correspondent
- **For SWIFTNet FIN service**
 - RMA filtering only applies to authenticated traffic
 - Non authenticated messages like MT999 can still be sent
 - Filtering on a BIC8 level
 - Optional granularity: message categories/types



Customer scheduling RMA milestones

- **Milestone C2:** demonstration of monthly live RMA usage
- **‘Your country’ C2 is ‘.....’ 2008**
- **Milestone C3:** completion of RMA activation
 - No more usage of MAC/PAC
 - No more usage of Bilateral Keys
- **‘Your country’ C3 is October to December 2008**



PKI pricing

PKI pricing (EUR)		
Item	One-Time	Recurring
Certificate	250	50
Security Officer		500
Shared Security Officers		400

