

Secure Information eXchange

- What needs to be considered?
- What solutions could be used to exchange sensitive information?



SGRP Special Interest Group "Secure Information eXchange (SIX)" in collaboration with ISSS
→ www.sgrp.ch/securex

Tobias Christen - Patrick Greuter - Anton Heer - Lukas Ruf - Martin Sibler - Walter Sprenger - Rudolf Studer - Erich Vogt



Agenda

1. Introduction
2. Approach
3. Evaluation Criteria
4. Secure Information eXchange (SIX) Patterns
5. Conclusions

Intro	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Approach	<input type="radio"/> <input type="radio"/>
Eval Criteria	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
SIX Patterns	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Conclusions	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>

Do you know the following solutions / products?

- Tumbleweed
- Axway
- FT Direct
- PrivaSphere
- IncaMail
- Totemo
- Trustmail
- SEEP
- PXE
- TNT securEdoc
- UPAQsend
- PostX
- Voltage Security
- WorkSmart
- DataMotion
- Postini
- MessageLabs
- MOVEit
- ...

Intro	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>
Approach	<input type="radio"/> <input type="radio"/>
Eval Criteria	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
SIX Patterns	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Conclusions	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>



Why do we need secure information exchange?

- Secure Information eXchange (SIX) is crucial when sensitive information is exchanged with business partners
- Different solutions exist but there is no one-size-fits-all solution available
- Solutions have to satisfy requirements on security, scalability, efficiency and usability simultaneously
- Our whitepaper proposes a set of design patterns for SIX that is based on a list of evaluation criteria devised by a special interest group (SIG) of SGRP in collaboration with ISSS

Intro	<input checked="" type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
Approach	<input type="radio"/> <input type="radio"/>
Eval Criteria	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
SIX Patterns	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Conclusions	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>



Objectives of the Special Interest Group (SIG)

- To deliver an overview of approaches and solutions for secure information exchange among business partners (business-to-business, B2B)
- To analyse solutions from the view point of end users and business contacts based on the evaluation criteria
- To develop design patterns to support an implementation
- To provide guidance and additional support material related to secure information exchange
- To indicate legal requirements to be considered for implementation

Intro	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Approach	<input type="radio"/> <input type="radio"/>
Eval Criteria	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
SIX Patterns	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Conclusions	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>



Approach – Patterns

- Target security officers of medium size and large corporations
- Balanced combination of "architectural overview" diagrams and explanatory text → design pattern characteristics
- Different solution designs - so called patterns - have been developed
- Patterns were developed according to the Open Security Architecture template and have been published on the OSA website - see <http://www.opensecurityarchitecture.org>

Intro	○ ○ ○
Approach	● ○
Eval Criteria	○ ○ ○ ○
SIX Patterns	○ ○ ○ ○ ○ ○
Conclusions	○ ○ ○ ○ ○



Approach – Controls

Intro	● ● ●
Approach	● ●
Eval Criteria	○ ○ ○ ○
SIX Patterns	○ ○ ○ ○ ○ ○
Conclusions	○ ○ ○ ○ ○

- Security officers who have to choose a solution to protect the exchange of sensitive information will require a set of evaluation criteria
- Elaborated on a set of non-overlapping solution attributes. A mapping table was developed to help security officers choosing a design pattern
- Challenge to secure "information exchange" between two corporate parties or between a corporate and its consumer clients requires a wide area of controls
- Controls were categorized in operational, technical and management controls. The underlying controls-catalogue NIST 800-53 was selected as it is freely available and can be easily mapped to ISO-27001



Evaluation Criteria

Intro	○ ○ ○
Approach	○ ○
Eval Criteria	● ○ ○ ○
SIX Patterns	○ ○ ○ ○ ○ ○
Conclusions	○ ○ ○ ○ ○

- Many different solutions are available to exchange sensitive information with business partners
- Each of these solutions fulfills different requirements and has specific characteristics
- In order to identify the appropriate solution for a specific business need, the solutions have to be grouped and classified
- Evaluation criteria can be used to group and classify the various solutions available
- These criteria are a subset of requirements that define the characteristics of a Secure Information eXchange solution and help to distinguish the different approaches and methods



Most important evaluation criteria

The following eight requirements have been identified as the most important evaluation criteria:

Evaluation Criteria	Definition
Data Size	The size / amount of information that will be exchanged
Frequency	How often does the data exchange happen
Setup Type	Can the solution be used immediately or is setup required (e.g. accounts)
Requires End User Provisioning	What does the user get / install prior to using the data exchange
Communication Relationship	Kind of communication relationship between users
Encryption Type	Confidentiality requirements of the data
User Identity Trust	How much trust is required for the user identity
Transparent solution	Is the user aware of the solution

- Intro
- Approach
- Eval Criteria
- SIX Patterns
- Conclusions

Patterns assessed against evaluation criteria

✓ = supported

(✓) = partly supported

Evaluation Criteria	Attribute Value	SIG SIX Patterns						
		E-Mail TLS Enforced	E-Mail TLS Opportunistic	AdHoc FileExchange	OneTime FileExchange	Realtime Collaboration	Board of Directors Room	USB Stick / Removable
Data Size	Small (< 1 MB)	✓	✓	✓	✓	✓	✓	✓
	Medium (1..35 MB)	✓	✓	✓	✓	✓	✓	✓
	Large (35 MB .. 500 MB)			✓		✓		✓
	Unrestricted (> 500 MB)					✓		✓
Frequency	daily	✓	✓	✓		✓		
	sporadic	✓	✓	✓	✓		✓	✓
	once		✓	✓	✓			✓
Setup Type	Self-Service			✓	✓			✓
	Administrator	✓	✓			✓	✓	(✓)
Requires End User Provisioning	none	✓	✓	✓	✓			
	Software					✓		
	Hardware					✓	✓	✓
	Training			✓	✓	✓	✓	
Communication Relationship	One-To-One	✓	✓	✓	✓	✓	✓	✓
	One-To-Many	✓	✓	✓		✓	✓	
	Many-To-Many					✓	✓	
Encryption Type	Gateway-To-Gateway	✓	✓					
	End user-To-End user			✓	✓	✓	✓	✓
	Content Encryption at rest			(✓)		(✓)	✓	✓
User Identity Trust	Self Registration / Anonymous			✓		(✓)		✓
	Verified Registration			✓	✓	✓	✓	
	Identity Federation	✓				✓		
Transparent Solution	No user interaction required	✓	✓					
	User interaction required			✓	✓	✓	✓	✓

- Intro
- Approach
- Eval Criteria
- SIX Patterns
- Conclusions



Other Evaluation Criteria

Intro	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Approach	<input type="radio"/> <input type="radio"/>
Eval Criteria	<input checked="" type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/>
SIX Patterns	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Conclusions	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>

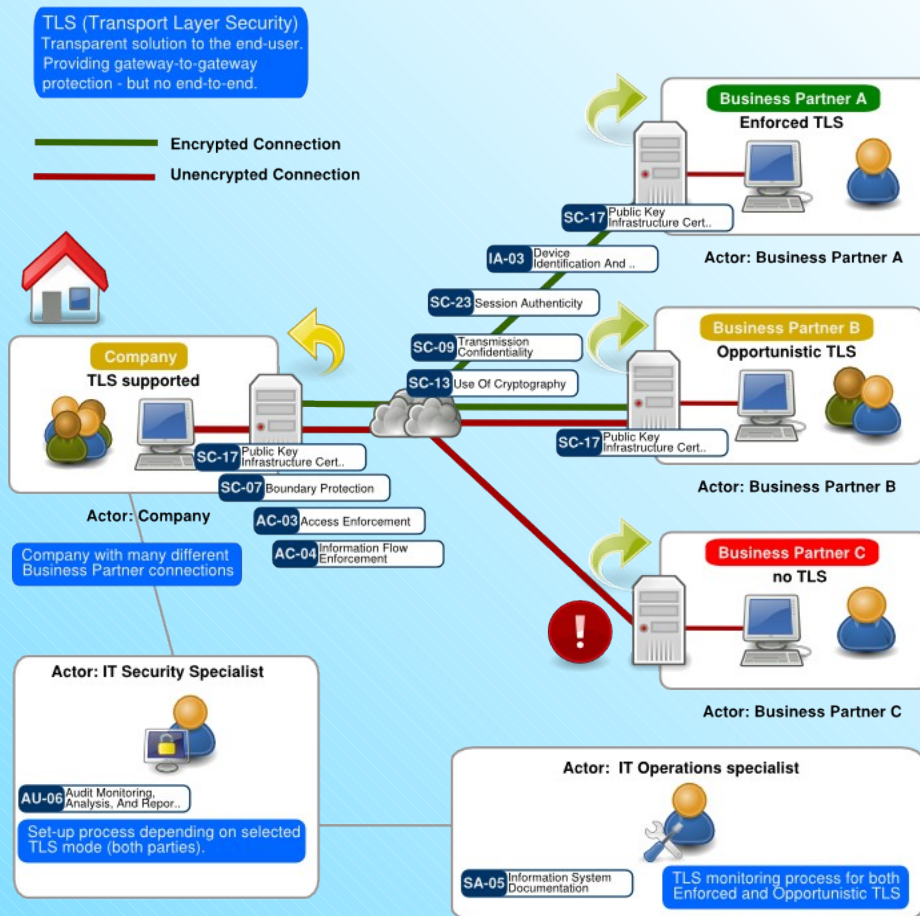
- Requirements regarding the data exchanged are:
 - Data format supported
 - Confidentiality and classification of the data
 - Integrity of the data in transit and at rest
 - ...
- Characteristics that further distinguish a solution are:
 - Availability of the solution
 - Credential transfer / Notification service (in-band / out-of-band)
 - Usability of the solution (skills required, handling and user acceptance)
 - Training need for users / administrators
 - Interface to other solutions
 - ...
- Confidentiality, integrity and availability of the data to be exchanged have to be guaranteed in a manner that they support the requirements of the business



E-mail TLS Enforced / Opportunistic

Intro	○ ○ ○
Approach	○ ○
Eval Criteria	○ ○ ○ ○ ○
SIX Patterns	○ ○ ○ ○ ○ ○
Conclusions	○ ○ ○ ○ ○ ○

Transport Layer Security (TLS) pattern for e-mail communication between companies particularly where the company has connections with many partners.





E-mail TLS Enforced / Opportunistic

Intro	<input type="radio"/> <input type="radio"/> <input type="radio"/>
Approach	<input type="radio"/> <input type="radio"/>
Eval Criteria	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>
SIX Patterns	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Conclusions	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>

Characteristics	Opportunistic TLS	Enforced TLS
Encryption principle	→ encryption likely	→ encryption ensured
E-mail transmission	E-mails are sent encrypted if TLS is supported	E-mails are only sent if encryption is possible
Encryption failure 1) behavior	If encryption fails, e-mails are sent unprotected	If encryption fails, no e-mail will be exchanged
TLS direction support	TLS could only be supported in one direction (e.g. outbound) or both	TLS must be supported in both directions (in- and outbound)
TLS requirements	No special TLS set-up required, even self-signed certificates are supported	TLS requirements must be met and only certificates issued by official CA (e.g. Verisign) are accepted. The “Common Name” field on the certificate must be set to the name that mail gateway
Configuration efforts	Default configuration and activated for all e-mail domains supporting TLS once set-up	Every business partner domain requires configuration, testing and monitoring
Costs	No additional costs once set-up	Additional costs to set-up and operate an Enforced TLS connection might result

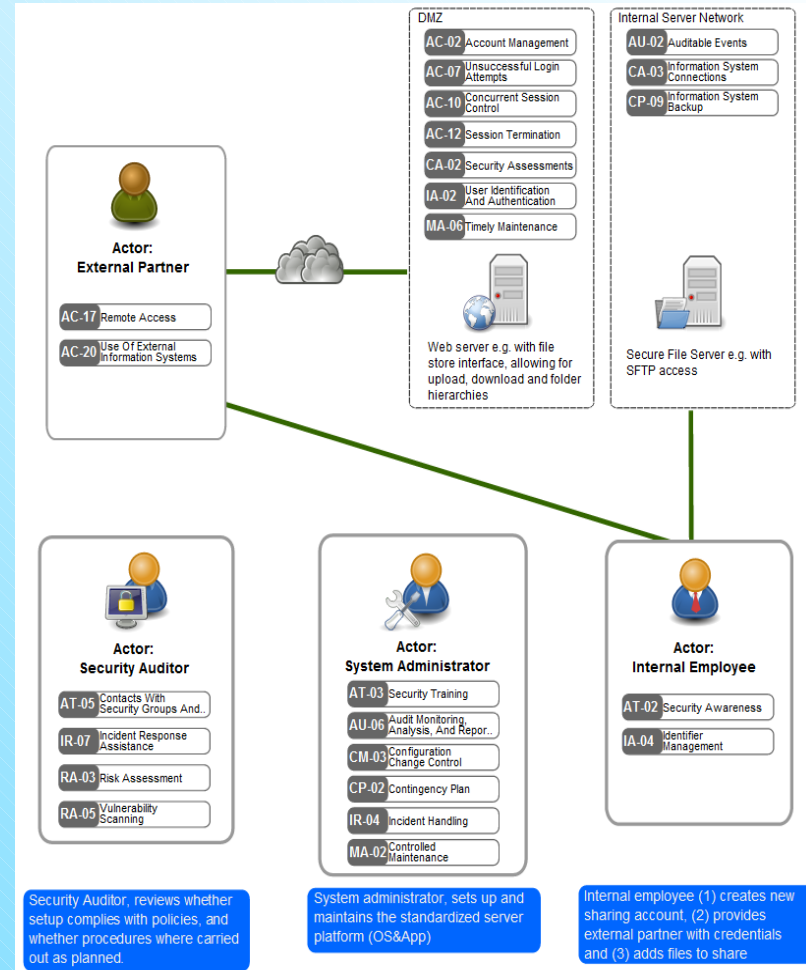
1) An encryption failure of the TLS connection is not very likely. Most encryption failures are caused by events that have an impact on the TLS server certificate. For example, it could be triggered by a change of e-mail infrastructure configuration (e.g. server name) or a change of the server certificate (e.g. expiration of certificate).



Ad-hoc File Exchange

- Intro
- Approach
- Eval Criteria
- SIX Patterns
- Conclusions

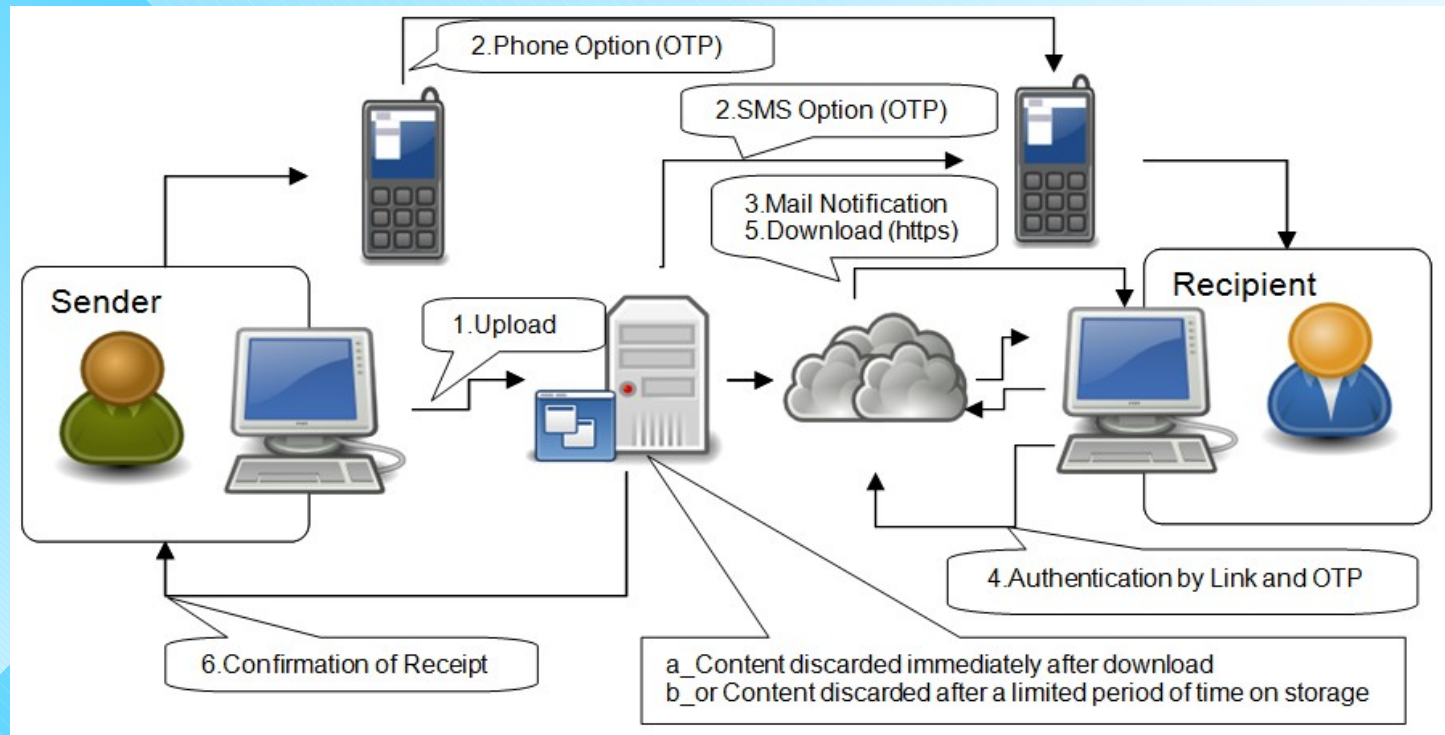
Two parties want to exchange confidential documents without the need of involving IT-departments.





One-time File Exchange (Secure e-Communication)

One-time File Exchange is easily applicable in case of spontaneous information exchange with a minimum of preconditions.

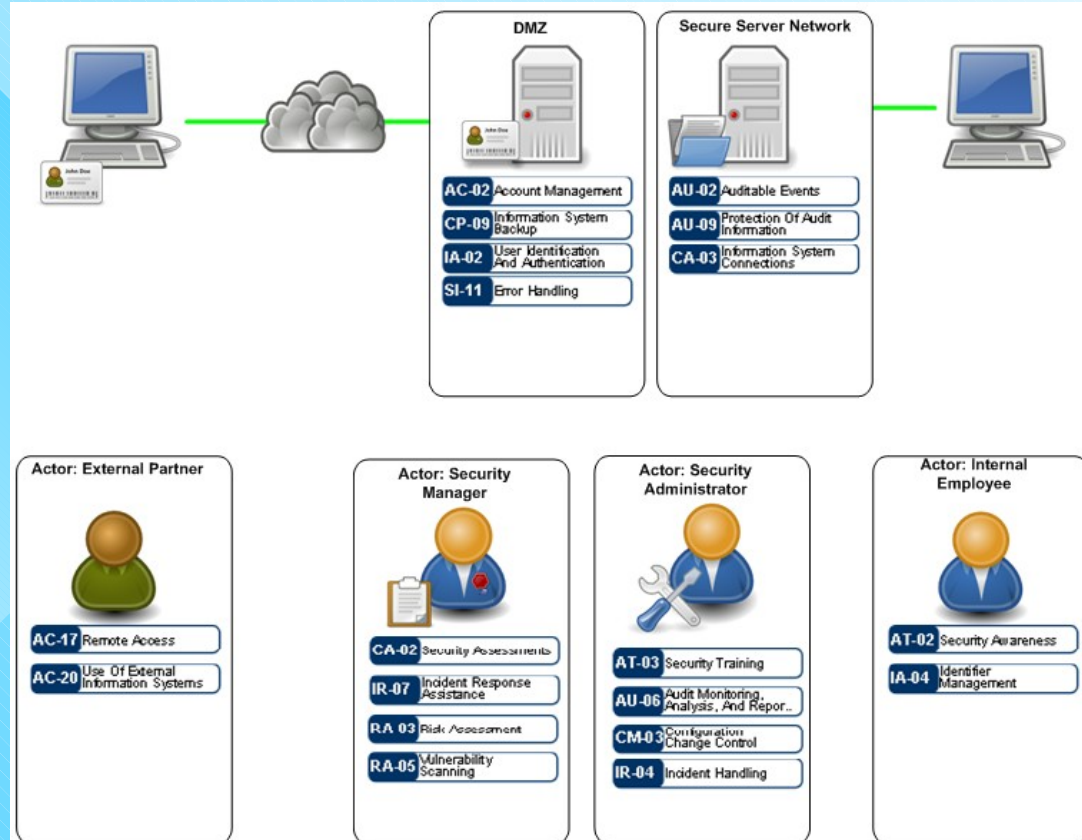


- Intro
- Approach
- Eval Criteria
- SIX Patterns
- Conclusions



Real-time Collaboration

Real-time collaboration pattern for working side by side on the same document.



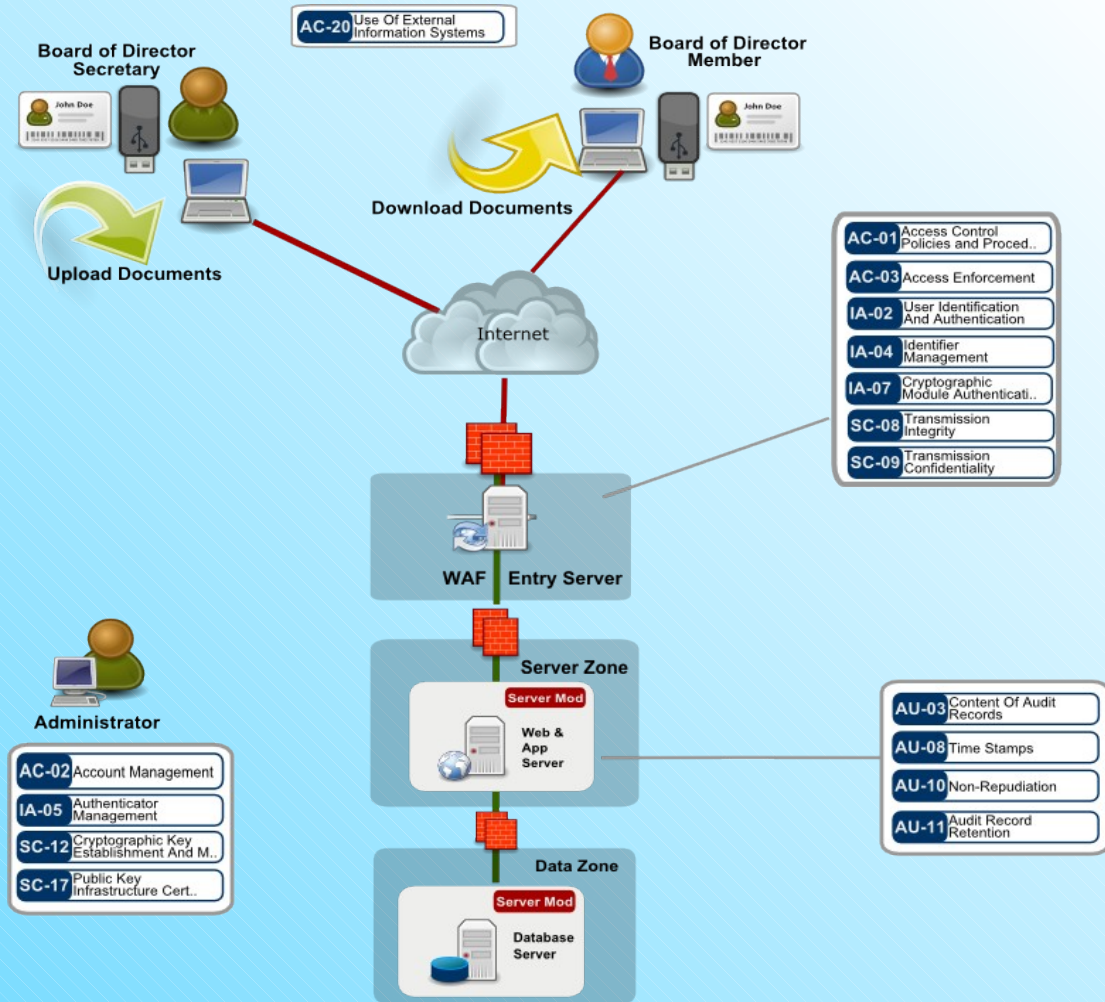
- Intro
- Approach
- Eval Criteria
- SIX Patterns
- Conclusions



Board of Directors Room

Intro	● ● ●
Approach	● ●
Eval Criteria	● ● ● ●
SIX Patterns	● ● ● ● ● ●
Conclusions	○ ○ ○ ○ ○ ○

Board of directors room for reading highly confidential documents on an un-trusted computer.





Conclusion – User Impact

- The success of a secure data exchange solution is based on the fact that users will not have to change their way of working significantly
- With an ideal solution, the users do not realize that they are exchanging data in a secure way
- All the security procedures are managed as background processes
- If a complex or sophisticated secure exchange solution is launched, users will avoid (or circumvent) such secure data exchange solutions

Intro	○ ○ ○
Approach	○ ○
Eval Criteria	○ ○ ○ ○
SIX Patterns	○ ○ ○ ○ ○ ○
Conclusions	○ ○ ○ ○ ○



Conclusion – Many solutions

- The market provides plenty of solutions that are sold as secure data exchange
- Every solution has a right to exist and often addresses a specific need
- The special interest group could not identify a secure data exchange solution that is accepted by the majority of the group members
- Some companies use a secure data exchange solution and expect their customers and contractors to use the same solution
- They are often not prepared to use the solution of their communication partner

Intro	○ ○ ○
Approach	○ ○
Eval Criteria	○ ○ ○ ○
SIX Patterns	○ ○ ○ ○ ○ ○
Conclusions	○ ○ ○ ○ ○



Conclusion – "Crystal Ball"

- Requirement to have secure communication is older than 10 years
- Costs = 1. Killer and Usability = 2. Killer
- Customer and Management awareness insufficient
- Feature creep hinders implementation
- New solutions appear and disappear fast
- Risk based approach is used → cost vs penalty
- Is a solution really practical and usable?
- ...

Intro	○ ○ ○
Approach	○ ○
Eval Criteria	○ ○ ○ ○
SIX Patterns	○ ○ ○ ○ ○ ○
Conclusions	○ ○ ○ ○ ○



Conclusion – Future

Intro	○ ○ ○
Approach	○ ○
Eval Criteria	○ ○ ○ ○
SIX Patterns	○ ○ ○ ○ ○ ○
Conclusions	○ ○ ○ ○ ○

- Technically it is possible to set up a secure data exchange solution
- The missing external pressure, the costs of the solution and the change of user behavior prevent the break-through of secure data exchange
- A solution that addresses the needs of the future does not only protect data in transit, but also ensures a secure data storage
- Provided that the data is protected on its own, it does not matter anymore whether the data is transmitted over or stored in an insecure network.
- Regulatory requirements, user-friendliness and flexibility regarding ICT-platforms will play a crucial role as driver for future development



Conclusion – Questions?

■ Are there any questions?

The whitepaper can be downloaded from
www.sgrp.ch/securex



SGRP Special Interest Group "Secure Information eXchange (SIX)" in collaboration with ISSS
→ **www.sgrp.ch/securex**

Tobias Christen - Patrick Greuter - Anton Heer - Lukas Ruf - Martin Sibler - Walter Sprenger - Rudolf Studer - Erich Vogt

Intro	○ ○
Approach	○ ○
Eval Criteria	○ ○ ○ ○
SIX Patterns	○ ○ ○ ○ ○ ○
Conclusions	○ ○ ○ ○ ○