

Secure Information eXchange



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

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

Whitepaper of the SGRP Special Interest Group "Secure Information eXchange (SIX)" in
collaboration with ISSS

© June 2011 by SIG-SIX

Abstract

Secure Information Exchange covers a wide area of different aspects to be considered. For a majority of companies all over the world, similar problems and challenges are faced when confidential or secret and/or sensitive information is to be shared among users of various legal entities. Currently, no unified standard exist that addresses all challenges. This whitepaper provides guidance and highlights a variety of possible solutions for further in-depth consideration.

Table of Contents

- 1 Introduction..... 3
 - 1.1 Document Structure 3
- 2 Approach 4
- 3 Evaluation Criteria 5
- 4 Secure Information Exchange Patterns 7
 - 4.1 E-mail TLS Enforced / Opportunistic..... 7
 - 4.2 Ad-hoc File Exchange 10
 - 4.3 One-time File Exchange (Secure e-Communication) 13
 - 4.4 Real-time Collaboration..... 15
 - 4.5 Board of Directors Room 17
 - 4.6 Removable Media / USB-Stick (Crypto) 19
- 5 Conclusion 22
- 6 Appendix 23
 - 6.1 Reference / Links 23
 - 6.2 Legal Notice 23
 - 6.3 Copyright 23

1 Introduction

Secure Information eXchange (SIX) is crucial for nearly all companies when sensitive information is exchanged among various legal entities including business partners. For a set of situations, secure e-mail by encrypted server-to-server channels is sufficient; for another, transport of data by encrypted USB devices meets the needs for confidentiality. However, currently no grand unifying solution exists in the wild that provides a feasible approach satisfying requirements on security, scalability, efficiency and usability simultaneously. This 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 the Sicherheitsgruppe Schweiz, (SGRP), Alumni Organization Information Security HSLU and the Information Security Society Switzerland (ISSS).

The Special Interest Group on Secure Information eXchange (SIG-SIX) (<http://www.sgrp.ch/securex>) addressed the following objectives:

- 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.

1.1 Document Structure

This document presents the results of the SIG-SIX. It structures these results according to the following outline:

- Chapter 2 describes the chosen approach.
- Chapter 3 introduces the evaluation criteria that are based on the experience of the SIG-SIX team-members. These criteria are provided in a table and mapped to the according design pattern.
- Chapter 4 presents the design patterns. Six design patterns are shown that cover the range from static, pre-setup information exchange mechanisms down to sporadic ad-hoc data transfer.
- Chapter 5 then concludes this document by emphasizing the challenges, approaches and derived results.

In the appendix, this document is completed by a list of relevant references and supportive links and a legal notice.

2 Approach

The SIG-SIX working group agreed to target security officers of medium size and large corporations with this publication.

As a consequence, a balanced combination of "architectural overview" diagrams and explanatory text is best suited to convey security best practices. The documentation structure is reflecting the well-known design pattern characteristics.

Different solution designs - so called patterns - have been developed as deliverables of the SIG "Secure Information eXchange". These patterns were developed according to the Open Security Architecture template and have been published on the OSA website - see <http://www.opensecurityarchitecture.org>

Security officers who have to choose a solution to protect the exchange of sensitive information will require a set of evaluation criteria. The working group has elaborated on a set of non-overlapping solution attributes. A mapping table was developed to help security officers choosing a design pattern.

The 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 (<http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf>) was selected as it is freely available and can be easily mapped to ISO-27001.

It is crucial that best practice patterns are not overloaded with control references, but to express only the minimal amount of controls. Reusing "modules", such as "DMZ", "secured server", helps to structure patterns and increase readability.

3 Evaluation Criteria

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.

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

Table 1: Definition of Evaluation Criteria

The patterns designed by the SIG-SIX were assessed against the identified evaluation criteria.

✓ = supported (✓) = partly supported

Evaluation Criteria	Attribute Value	SIG SIX Patterns						
		<u>E-Mail TLS Enforced</u>	<u>E-Mail TLS Opportunistic</u>	<u>AdHoc FileExchange</u>	<u>OneTime FileExchange</u>	<u>Realtime Collaboration</u>	<u>Board of Directors Room</u>	<u>USB Stick / Removable Media</u>
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			✓	✓	✓	✓	✓

Table 2: Patterns assessed against the Evaluation Criteria

As there are many different solutions available to address the various business needs, there are also many additional requirements that can be used to describe the characteristics of a solution.

Requirements regarding the data exchanged are:

- Data format supported
- Confidentiality and classification of the data
- Integrity of the data in transit and at rest
- Backup of transferred data
- Archiving of the data

Characteristics that further distinguish a solution are:

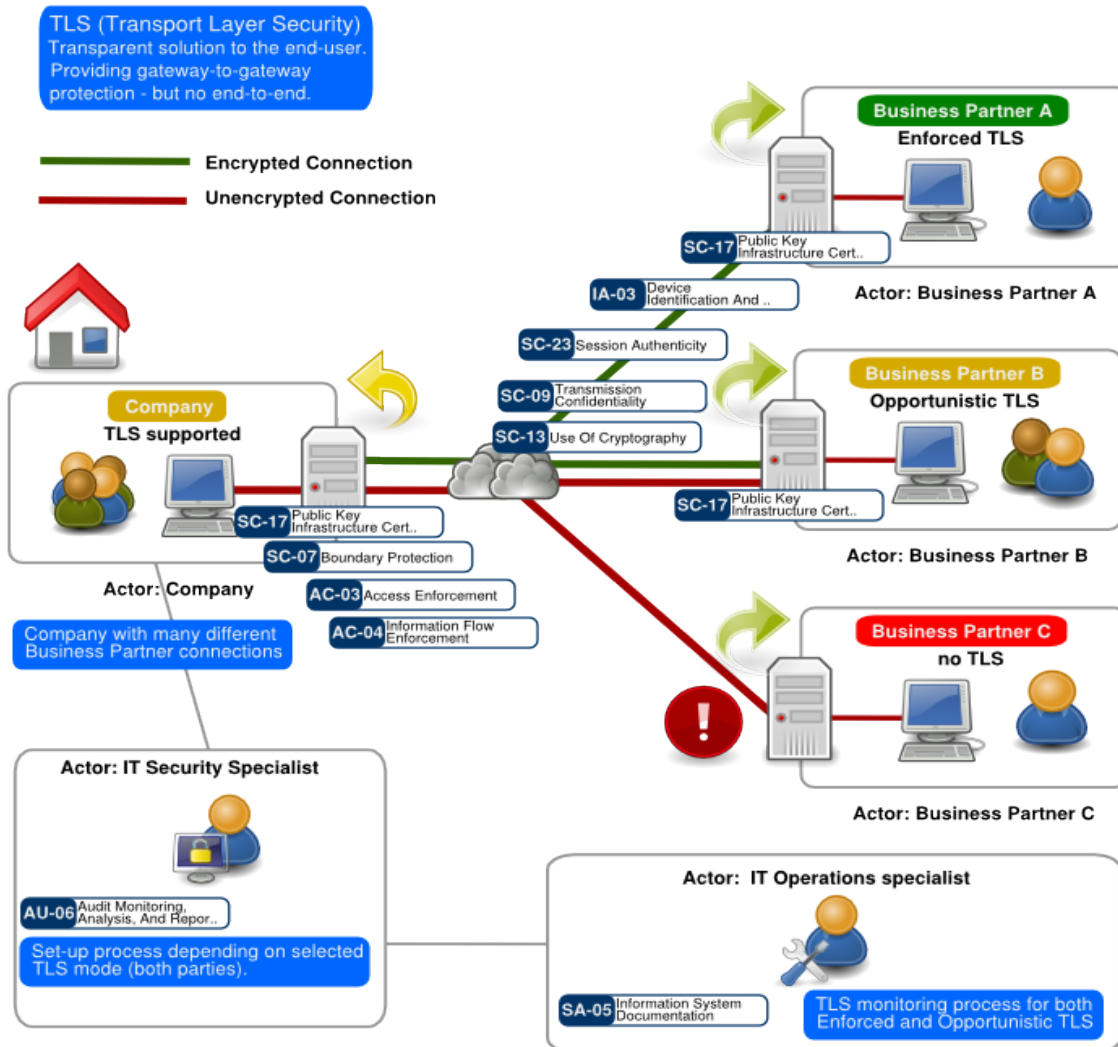
- Availability of the solution
- Credential transfer (in-band / out-of-band)
- Notification service (in-band / out-of-band)
- Usability of the solution (skills required, handling and user acceptance)
- Training need for users / administrators
- Interface to other solutions
- Complexity of the system infrastructure
- Accountability of the transaction, including end user logs / audit trail
- Service / Solution Ownership (in-house, partner, third party)
- Need for maintenance
- Decommissioning efforts required (tear down / clean up)
- Supported Standards (e.g. AES encryption)
- Compliance with legal requirements / laws (e.g. UK data privacy act)

The selection of the requirements and characteristics to compile the evaluation criteria of a solution is an important step in order to ensure that the risks related to the solution are mitigated. Consequently, the 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.

4 Secure Information Exchange Patterns

4.1 E-mail TLS Enforced / Opportunistic

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



Description: Companies have to assess the methods used to exchange sensitive information with business partners. Based on current legislation in many countries, they must ensure that sensitive information is exchanged with business partners via a secure communication channel. One of the most user-friendly and very efficient / secure ways to secure e-mail communication is to activate TLS (Transport Layer Security) on the mail gateways of both communication parties. This method is fully transparent to the end-user and protection is applied on the mail gateway / infrastructure level.

Processes to consider:

- TLS set-up process depending on selected TLS mode
- TLS operations process – monitor that Enforced TLS connections are operational
- TLS monitoring process to verify level of encryption of Opportunistic TLS connections

An initial set-up effort is required to configure TLS protection on the mail gateway (MTA) of both business partners. Additionally, processes need to be defined to monitor continuous protection of such a connection. Two different modes of TLS are available, Opportunistic TLS and Enforced TLS, with the following characteristics:

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

Table 3: Enforced TLS vs Opportunistic TLS

Further aspects have to be considered in the design approach if the mail gateway (MTA) is outsourced to a third party (e.g. Postini, MessageLabs). In this case, certain requirements of the outsourcing partners have to be met for Enforced TLS connections. For example, certificates have to be issued by trusted CA's and meet requirements concerning the "Common Name". Moreover, it also has to be ensured that TLS protection is ensured in both directions from an internal MTA of one company to the internal MTA of the other company. Often, TLS protection is only provided from one company to the e-mail outsourcer of the other company and sent reply e-mails are not TLS protected at all. This is the case because the outsourcer's MTA provides TLS per default, but the company's internal MTA does not have TLS activated.

Assumptions: Protection of the e-mail communication at the infrastructure level (gateway-to-gateway) provides sufficient protection. No end-to-end protection is required.

Typical challenges: Not every mail gateway (MTA) of communication partners supports TLS (Transport Layer Security). Furthermore, TLS might be supported, but is not configured properly. Additional challenges exist if an e-mail outsourcer is involved in TLS connections. Not all MTAs are able to meet the additional requirements that outsourcers might have in order to establish an Enforced TLS connection.

Indications: Transparent solution that requires no end-user interaction in order to have protection of the e-mail communication.

Contra-indications: E-mail communication must be protected from the sender's computer to the receiver's computer (end-to-end protection) to ensure that only the intended recipient has access to the information.

Resistance against threats: E-mail communication is protected over the Internet in order to prevent eavesdropping of confidential information. No end-to-end protection. A number of residual risks remain with this pattern:

- Confidentiality for e-mail communication is not guaranteed inside the company's intranet. In addition, confidentiality in an end-to-end communication cannot be ensured if a third party (outsourcer) is providing the e-mail gateway functionality (MTA). In this case the TLS communication is terminated at the mail gateway of this third party and the e-mails can be read by the third party. It has to be ensured that e-mail communication is also protected from the third party to the company's internal mail server.
- Loss of availability- The risk that e-mail communication is blocked between business partners exists for Enforced TLS connections if encryption is not possible. Continuous monitoring of Enforced TLS connections is required to identify encryption failures. Procedures have to be in place to temporarily remove the Enforced TLS policy in order to re-establish the e-mail communication until the technical difficulties have been resolved which caused the encryption failure.
- No 100% encryption guarantee. Opportunistic TLS does not guarantee 100% security – if encryption is not possible, e-mails are sent in clear text. Therefore, monitoring of such connections is required to prove that appropriate protection is provided by Opportunistic TLS.
- TLS stack vulnerability- E-mail communication could be eavesdropped due to vulnerabilities in the TLS communication stack.
- Identification of MTA- In case of Opportunistic TLS the authentication of the receiving mail server (MTA) cannot be guaranteed as self-signed certificates are accepted.

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).

References:

- OpenSSL: <http://www.openssl.org/docs/apps/openssl.html>
- RFC 5246 - The TLS Protocol v1.2 : <http://www.rfc-editor.org/rfc/rfc5246.txt>
- RFC 3207 - Secure SMTP over TLS: <http://www.rfc-editor.org/rfc/rfc3207.txt>
- RFC 2821- Simple Mail Transfer Protocol: <http://www.rfc-editor.org/rfc/rfc2821.txt>

Related patterns: E-mail TLS with MTA outsourcing (Pending)

Classification: e-mail communication

Release: April 2010

<http://www.opensecurityarchitecture.org/cms/library/patternlandscape/275-pattern-email-transport-layer-security-tls>

Author(s): Martin Sibling;

pattern was created based on the result of the SGRP Special Interest Group "Secure Information Exchange"

Reviewer(s): Tobias Christen

Control details:

[AC-03 Access Enforcement](#)

[AC-04 Information Flow Enforcement](#)

[AU-06 Audit Monitoring, Analysis, And Reporting](#)

[IA-03 Device Identification And Authentication](#)

[SA-05 Information System Documentation](#)

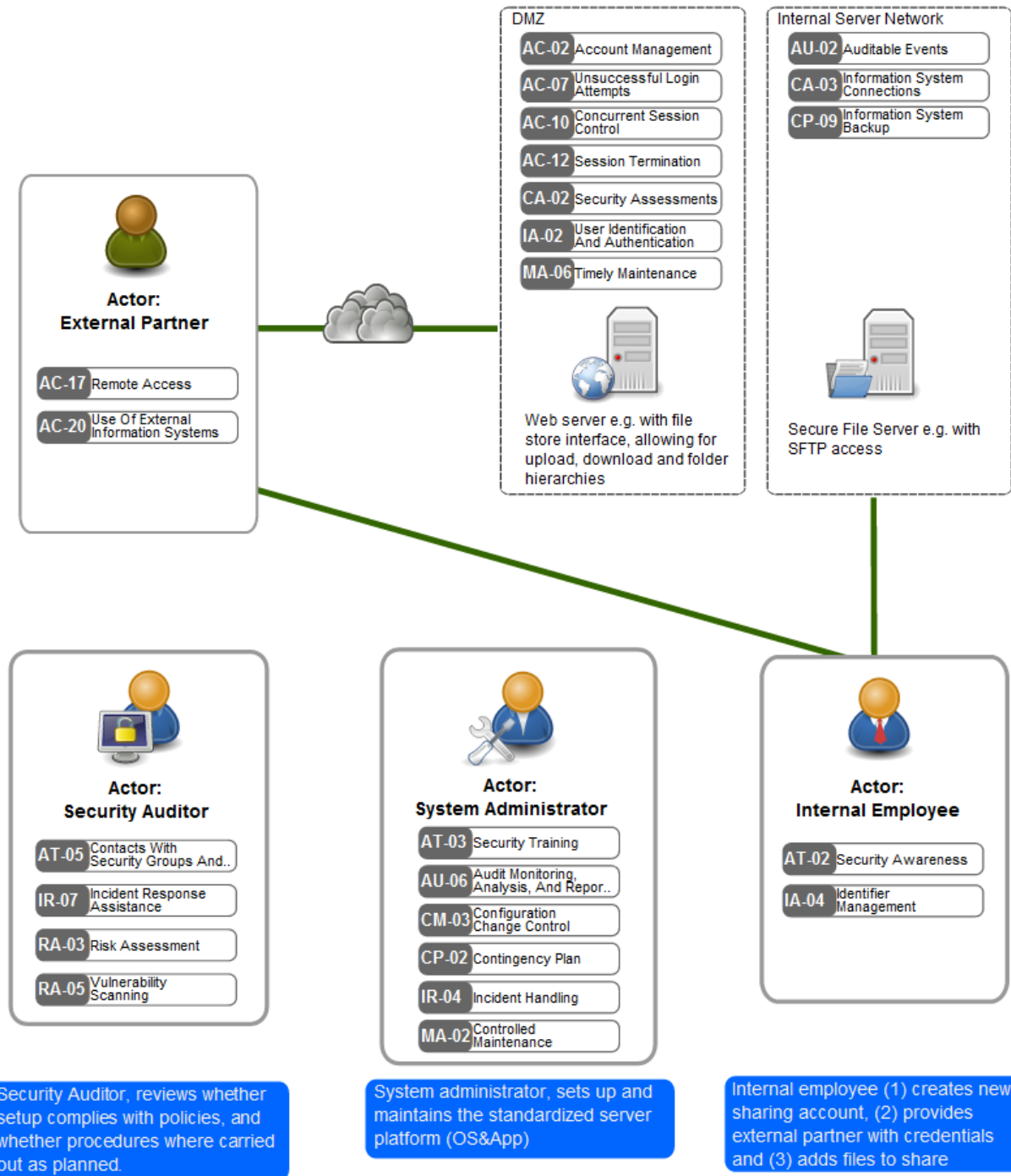
[SC-07 Boundary Protection](#)

[SC-09 Transmission Confidentiality](#)

[SC-13 Use Of Cryptography](#)

4.2 Ad-hoc File Exchange

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



Description: Two parties (for example a supplier and his customer) want to exchange confidential documents. They are both connected via internet but have no pre-established common IT infrastructure, therefore the sharing needs to be ad-hoc enabled.

We are describing a pattern here that supports a scenario where only business users interact in the file exchange workflow. Neither an approval / setup process, nor any trust-accreditation processes shall be required. Business users should therefore be able to help themselves and activate the sharing with as little as 2 or 3 steps.

Technical Design Considerations: The size of the data to be shared has to be considered. If the size is too big (e.g. several gigabytes), then an introduction of storage and bandwidth quota needs to be considered to minimize impact on other users.

To keep the technical solution setup as simple as possible, a single “secure-data-sharing” application would be preferred. Such solutions can either be hosted in the corporate data centre or could be acquired as SaaS.

Assumptions: As it has to be assumed that the data being shared can be classified as confidential, strong encryption is required by most corporate security policies. Data on the move as well as data at rest should therefore be encrypted.

In an ad-hoc scenario it is unlikely that digital rights management solutions (with water marking, and copy prevention) would be required.

Typical challenges: What are issues to expect?

To overcome typical usability and acceptance issues. The solutions to the problem of ad-hoc file exchange need to be able to meet the following challenges.

- Very low effort to setup / use the solution
- pay as you go licensing, pricing model
- guarantee of privacy and confidentiality protection even if the solution is hosted by a third party

Indications: The discussed pattern matches best if the following indicators can be found:

- Business driven: business decides ad-hoc when and where the solution is required / used
- Simplified user interface also allows staff members with low IT affinity to use the solution
- Low integration costs
- Identity federation with partner is not established
- Business unit is data owner, IT does not act as data owner custodian, business unit staff members can decide who needs access, when and where
- Audit trail needs to be available

Contra-Indications: Strong integration into document management workflow requires a single repository for internal and external collaboration. High real-time collaboration requirements. These contra-indicators would rather point to a pre-setup data-sharing solution with identity federation.

Resistance against threats: The following threats are taken into account in the design of this pattern:

- Loss of business opportunities due to delays in IT-Setup: Ad-hoc sharing allows business users to decide instantly which documents are shared with whom
- Irrational risk acceptance to save setup costs: To avoid the syndrome where business managers take the risk to violate regulations and may violate the confidentiality, it is important to have an opportunity where setting up a secure file sharing does not incur high setup-project costs. Being able to benefit from a pay-as-you-go SaaS setup mitigates this risk.

Residual risks that are not mitigated: Scenarios where documents that are embedded in a complex sign-off and processing workflow are typically not well-served with an ad-hoc setup.

Related Business Processes Considerations: The business processes that involve sharing confidential data will need to address the following issues:

- Data classification: the person that shares the data needs to be aware of the data classification and the associated duty of care.
- Data ownership: the person that shares the data needs to own the data or at least be the custodian of the data
- Partner identification: the person that shares the data needs to be able to identify the partner securely

Reference / Related Use Cases: What are related Use Cases?

One time file exchange - very closely related pattern that puts the focus on a specific way on how to inform recipients.

Release: February 2010

<http://www.opensecurityarchitecture.org/cms/en/library/patternlandscape/276-pattern-secure-ad-hoc-file-exchange>

Author(s): Tobias Christen;

pattern was created based on the result of the SGRP Special Interest Group "Secure Information Exchange"

Reviewer(s): Patrick Greuter

Controls:

[AC-02 Account Management](#)

[AC-07 Unsuccessful Login Attempts](#)

[AC-10 Concurrent Session Control](#)

[AC-12 Session Termination](#)

[AC-17 Remote Access](#)

[AC-20 Use Of External Information Systems](#)

[AT-02 Security Awareness](#)

[AT-03 Security Training](#)

[AT-05 Contacts With Security Groups And Associations](#)

[AU-02 Auditable Events](#)

[AU-06 Audit Monitoring, Analysis, And Reporting](#)

[CA-02 Security Assessments](#)

[CA-03 Information System Connections](#)

[CM-03 Configuration Change Control](#)

[CP-02 Contingency Plan](#)

[CP-09 Information System Backup](#)

[IA-02 User Identification And Authentication](#)

[IA-04 Identifier Management](#)

[IR-04 Incident Handling](#)

[IR-07 Incident Response Assistance](#)

[MA-02 Controlled Maintenance](#)

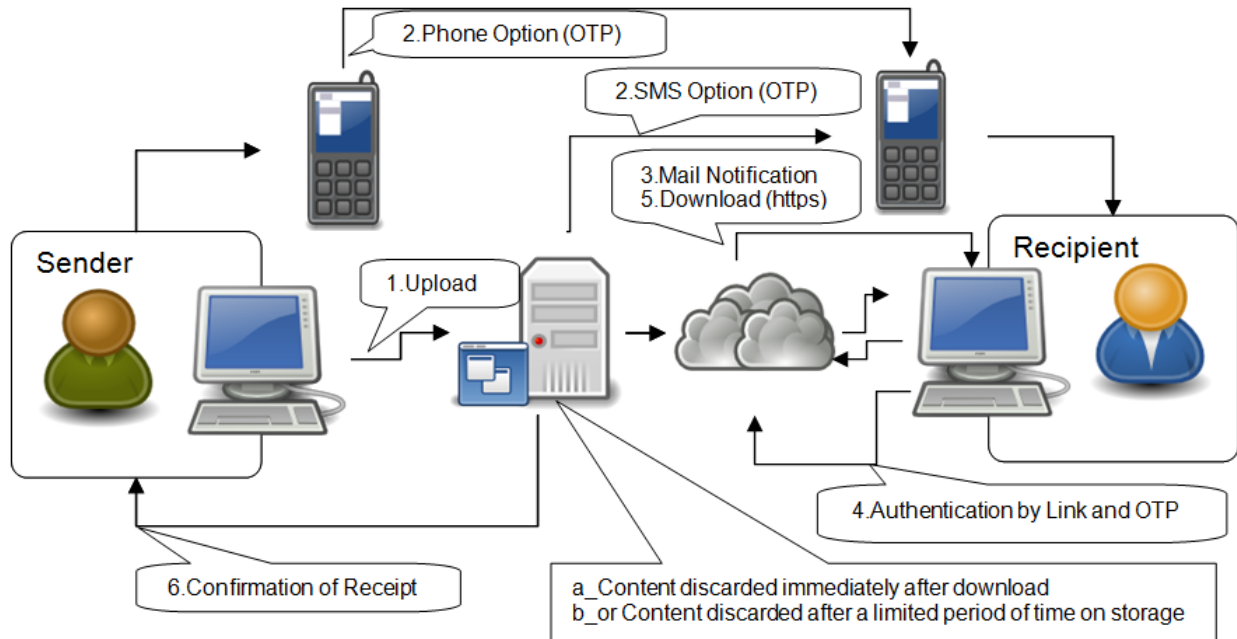
[MA-06 Timely Maintenance](#)

[RA-03 Risk Assessment](#)

[RA-05 Vulnerability Scanning](#)

4.3 One-time File Exchange (Secure e-Communication)

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



Description: This pattern enables a user (sender) to transfer single files securely to an internal or external recipient. This pattern emphasizes simplicity and does not require major technical preconditions. The security of data transfer is based on a two-channel-approach. Internet and an independent network (Telephony) assure a sufficient separation of environments.

Technical Design Approach: Data to be transferred is temporarily stored on a transfer-server, accessible by recipients (via a link). The recipient is authenticated with the help of the OTP information, which is generated by the now described system. The OTP information is transmitted to the recipient by the system via SMS (short mobile message on mobile phones) (or optionally via voice communication). Hence two independent channels (SMS and e-mail) assure mitigation of eaves-dropping and simple man in the middle attacks.

Assumptions: A simple process allows an ad-hoc file transfer to a technically unknown environment. The limitation to a single file and a single recipient is regarded as sufficient for common business requirements. The need for an inexpensive and simple solution, requiring a minimum of setup procedures, is considered.

Typical challenge:

- Protection of confidentiality in case of sensitive business information (Privacy, health data, DPA, banking regulations, ongoing negotiations or other reasons for protection).
- Reasonable opportunity to obtain a high level of protection by a simple, comprehensible and transparent communication process in case of unknown communication means (e.g. system components).
- Acceptable robustness against accidental misuse or deliberate attacks.

Indication:

- Secure and single transfer of one file to one recipient.
- Low initial and operational costs.

Contra-Indication:

- Secure transfer of more than one file to several recipients.
- Repeated access to the source (file stored).
- The points above are neither possible nor within scope due to the simplicity of the solution design.

Threats:

- Access to data transferred by misuse of link and OTP (physical access to recipient's equipment or eavesdropping SMS or faking phone call).
- Loss of file due to handling errors, loss of OTP or late access.
- Compatibility issues caused by network infrastructure (exceptional).

Residual Risk:

- Basically the loss of data. That is to be considered in case of handling errors, time limits exceeded etc.
- Deliberate attacks or an attempted misuse could cause a loss of data or a very unlikely disclosure of data.

Controls:

- Appropriate and careful handling of OTP (Options phone or SMS, confidentiality of OTP).
- Bilateral tracking of transfer process (system based and implemented feedback messages).

References to some applicable OSA/NIST Controls:

[AC-01 Access Control Policies and Procedures](#) (internal & external user instructions, guidance)

[AC-20 Use Of External Information Systems](#) (by dissemination of user instructions, guidance)

[AT-02 Security Awareness](#) (is part of user instructions, guidance)

[AU-02 Auditable Events](#) (server-related audit trail is implemented and communication process generates immediate confirmations)

[IA-02 User Identification And Authentication](#) (is performed per each single event of information exchange)

[IA-06 Authenticator Feedback](#) (is kept to an absolute minimum)

[SC-08 Transmission Integrity](#) (is assured by using https)

[SC-09 Transmission Confidentiality](#) (is assured by using https)

Process flows:

- Initial information by e-mail and / or phone.
- Perform sender and checking activities.
- Perform recipient's activities.

Reference / Related Use Cases:

See "Ad-hoc Secure File Exchange"

Roles and Responsibilities (OSA Actors):

- Sender: duty to inform recipient and to manage initial steps (according to instruction manual)
- Recipient: duty to act according to instruction manual
- Note: Initially the sender acts as an internal instance (service owner or eventually service provider). Afterwards the original recipient (usually an external instance) is also able to act as a sender.

Related Regulations:

Data protection law, banking regulations, policies, companies' own requirements, etc.

Classification / Parameter:

- Transfer of sensitive data (single-data-file).
- Transfer of one file to one recipient.
- Limited file size (range of 10 to 100 MB, depending on infrastructure).

Release: March 2010

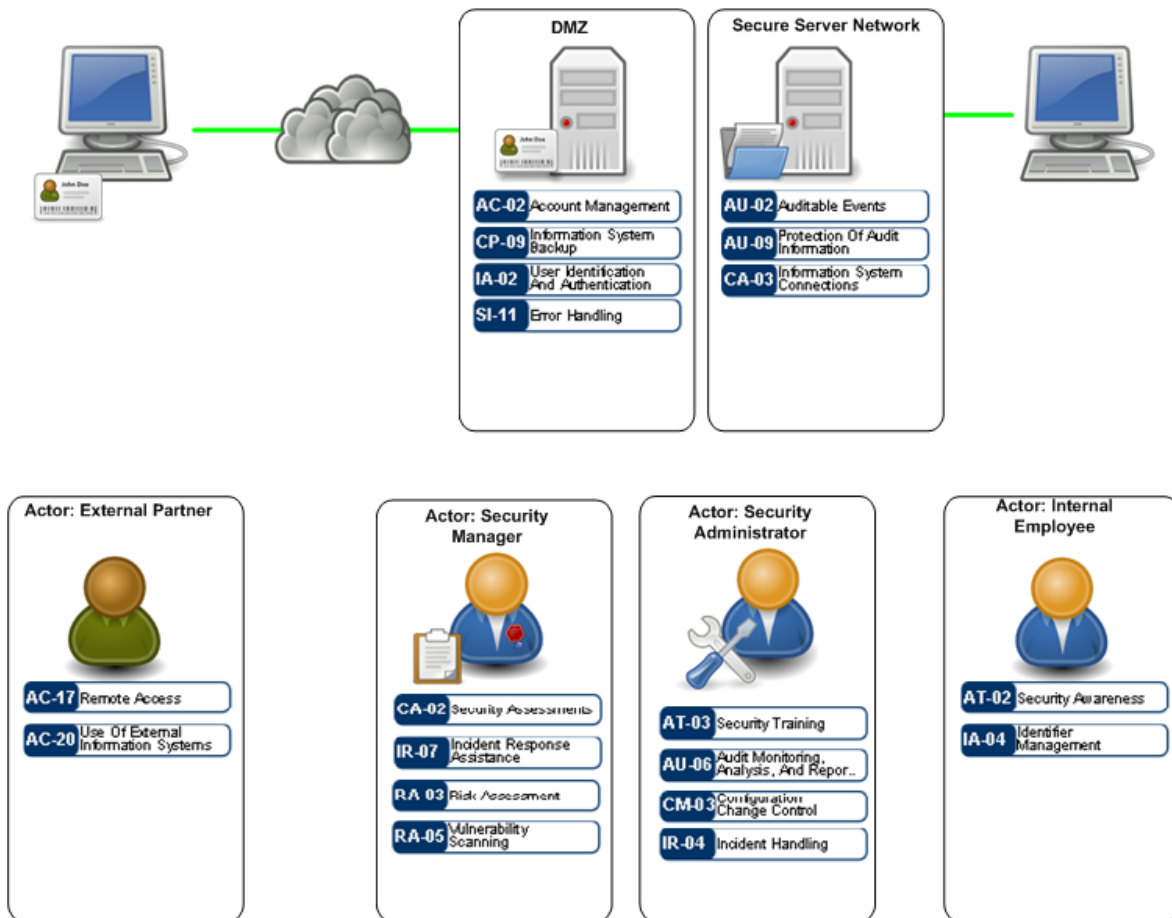
Author(s): Anton Heer;

pattern was created based on the result of the SGRP Special Interest Group "Secure Information Exchange"

Reviewer(s): Tobias Christen

4.4 Real-time Collaboration

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



Description: Real-time collaboration has different purposes. The most common case is when different users (internals and externals) have to work on the same document at the same time. Other requirements are the merging of different document versions as well as fast and save synchronization. This is focused on in this pattern.

Based on the requirements that a user has, he gets only access permission to specific files or folders, therefore a process for user provisioning over the whole life cycle is needed.

This pattern is only focused on business requirement regarding collaboration on business documents i.e. project maps, strategy plans and so on.

Assumptions: It has to be assumed that the highest classification of the shared information will be confidential and so the communication channel and the storage place should therefore be encrypted. There is also a high technical requirement to the availability of the document which is the working target of the real-time collaboration on documents. Another aspect is capacity of the available storage; it has to be assumed that documents are growing during the period of collaboration till the document receives the final status.

Typical challenge: Real-time collaboration on business documents is not an ad-hoc solution; there are permanent user accounts in conjunction with access to dedicated storage places. The challenge will be the user provisioning, to ensure that a user account is bound to a contract or agreement and will be maintained according to the user life cycle process.

Indications: The following indicators best support this case:

- Simple process for user provisioning
- Easy to use browser basis interface
- The business is the information owner and decides who gets access to which information
- Strong two-factor authentication by using MTAN, or token (i.e. OTP, certificates)
- Audit trails have to be available

Contra-Indications: The following contraindications have to be considered:

- Shared responsibilities regarding user provisioning between IT and business
- Central repository for internal and external users
- Traceability of the document changes

Technical Design Approach: The number of different users with access permission to dedicated files needs to be considered. This will have an impact on the user management process as well as on the storage and bandwidth between the two parties.

Threats: The following threats have to be considered:

- Files can be stored by external users which contain malicious code
- User obtains too much permission or wrong folder access
- Versioning conflict if too many users work on the document at the same time

Residual Risk: The residual risk that always will remain is unmanaged client security of the external partner (data leakage). Even this risk varies depending on whether it is a client of a trusted company or a client of a private person.

Process flows: The most important process is, as mentioned above, the user provisioning workflow. This workflow will be strongly influenced by information classification and information ownership.

Reference / Related Use Cases: Web conference is one use case which is very similar to this case. The only difference is the timeframe. In contrast to a web conference or an ad-hoc solution, real-time collaboration on documents is used over a longer time period.

Related Regulations

- Data Privacy Act
- Internal regulations (i.e. information classification)

Classification / Parameter

- End-to-end encryption
- Traceability
- User account management

Release: May 2010

<http://www.opensecurityarchitecture.org/cms/en/library/patternlandscape/281-draft-pattern-realtime-collaboration>

Author(s): Patrick Greuter;

pattern was created based on the result of the SGRP Special Interest Group "Secure Information Exchange"

Reviewer(s): Lukas Ruf

Controls: Controls related to systems:

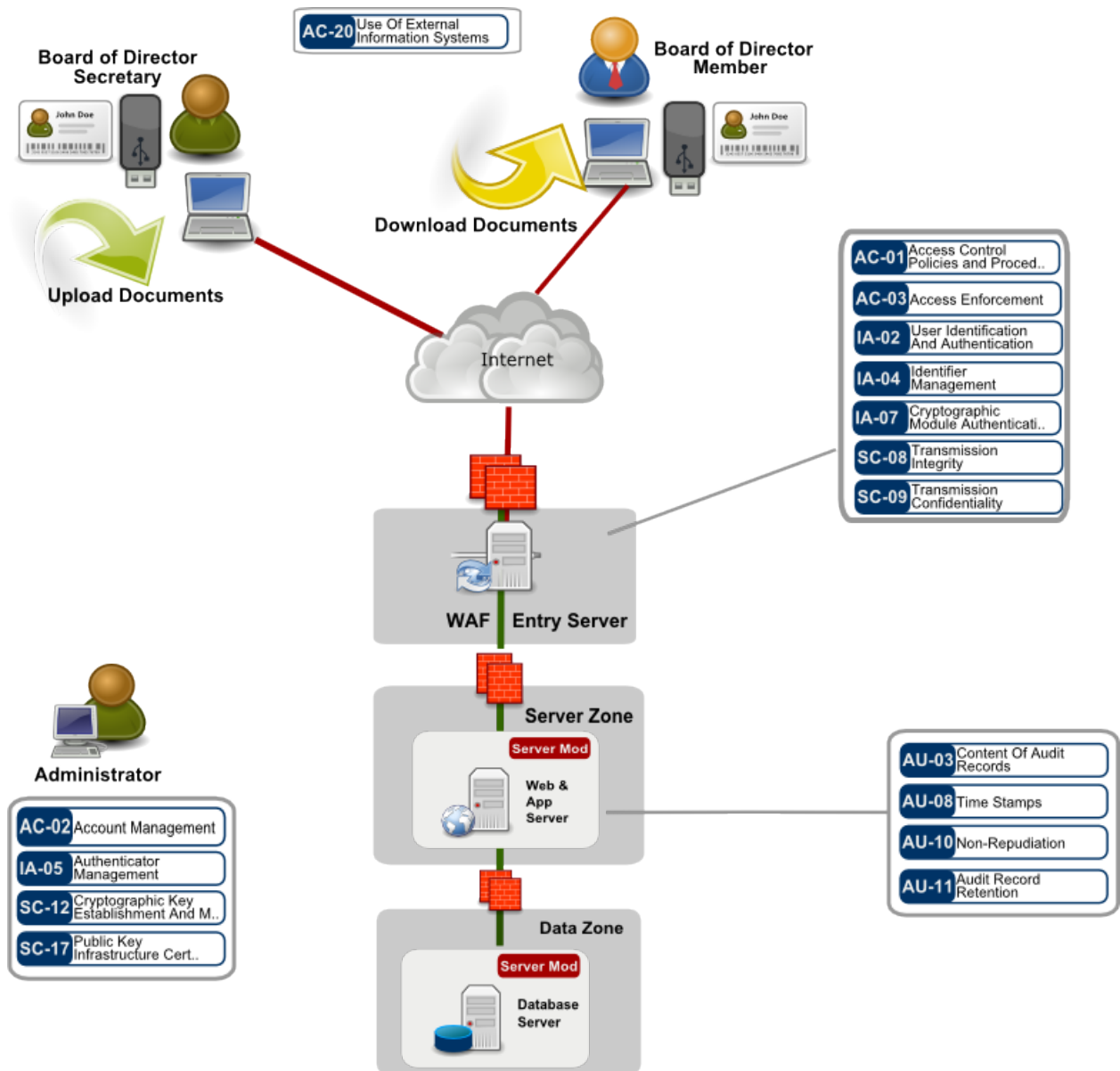
[AC-02 Account Management](#)
[AU-02 Auditable Events](#)
[AU-09 Protection Of Audit Information](#)
[CA-03 Information System Connections](#)
[CP-09 Information System Backup](#)
[IA-02 User Identification And Authentication](#)
[SI-11 Error Handling](#)

Controls related to persons:

[AC-17 Remote Access](#)
[AC-20 Use Of External Information Systems](#)
[AT-02 Security Awareness](#)
[AT-03 Security Training](#)
[AU-06 Audit Monitoring, Analysis, And Reporting](#)
[CM-03 Configuration Change Control](#)
[IA-04 Identifier Management](#)
[IR-04 Incident Handling](#)
[RA-03 Risk Assessment](#)
[RA-05 Vulnerability Scanning](#)

4.5 Board of Directors Room

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



Description: The board of directors needs access to meeting protocols, the agenda and other highly confidential information. Any computer may be used, even un-trusted or compromised computers. The documents accessible are highly confidential and no traces of documents shall be found on the computer. It must not be possible to download the documents in clear text or to print the documents. Detailed audit functionality shows which user has read which document and when. All documents are stored in the PDF format.

The following technical design aspects need to be considered:

- The solution should be supported by multiple operating systems (Windows, OS X, Linux)
- A USB stick is delivered to the members of the board and to its secretaries
- The USB stick contains the "board of directors' room" applications and a smartcard component comprising a certificate for cryptography operations
- Public key infrastructure is required to encrypt the PDF documents exchanged via the "board of directors" application.
- The "board of directors room" application will load a hardened web browser and a hardened PDF viewer from the USB stick to access the trusted and preconfigured web server
- The USB stick should be updated automatically by the "board of directors room" web server

Uploading documents: The secretary creates a PDF document and encrypts the document with the public key of every director. The encrypted PDF document is uploaded to the server.

Downloading documents: The board of director connects the USB stick to a PC. The hardened browser is started automatically and prompts for the PIN. The PIN is used to allow the web browser to access the certificate on the stick and to login to the web server. Encrypted PDFs can now be downloaded to the USB stick and stored. For viewing the PDFs, the PDF viewer will decrypt the PDF with the private key of the user certificate stored in the smartcard component.

Assumptions: Only small user base – 10-30 users expected. The computers of the board secretaries, where the documents are created, are secure.

Indications: Easy to use, but highly secure. Documents can be read on any un-trusted computer, it is assumed a Trojan horse is present on the computer where the documents are read. Documents are also encrypted when downloaded to the USB stick.

Contra-Indications: It is not an Ad-hoc solution, a USB stick is delivered to the users in the setup phase. The solution is practical only for a small number of users.

Resistance against threats: The solution is resistant against generic Trojan horses on the un-trusted computer where the board of directors reads the documents. The "board of directors room" application is secured against any web application threats according to OWASP.

A number of residual risks remain with this pattern:

- A board member taking screenshots and printing, mailing or saving the screenshots
- A board member handing the secure device over to other persons
- A specific Trojan Horse attacking this specific device (USB stick with hardened browser)

Related patterns: Other SIX patterns

Classification: File Exchange

Release: October 2010

<http://www.opensecurityarchitecture.org/cms/en/library/patternlandscape/292-draft-pattern-board-room>

Author(s): Walter Sprenger,
pattern was created based on the result of the SGRP Special Interest Group "Secure Information Exchange"

Reviewer(s): Martin Sibling

Controls:

[AC-01 Access Control Policies and Procedures](#)

[AC-02 Account Management](#)

[AC-03 Access Enforcement](#)

[AC-20 Use Of External Information Systems](#)

[IA-02 User Identification And Authentication](#)

[IA-04 Identifier Management](#)

[IA-05 Authenticator Management](#)

[IA-07 Cryptographic Module Authentication](#)

[SC-08 Transmission Integrity](#)

[SC-09 Transmission Confidentiality](#)

[SC-12 Cryptographic Key Establishment And Management](#)

[SC-17 Public Key Infrastructure Certificates](#)

[AU-03 Content Of Audit Records](#)

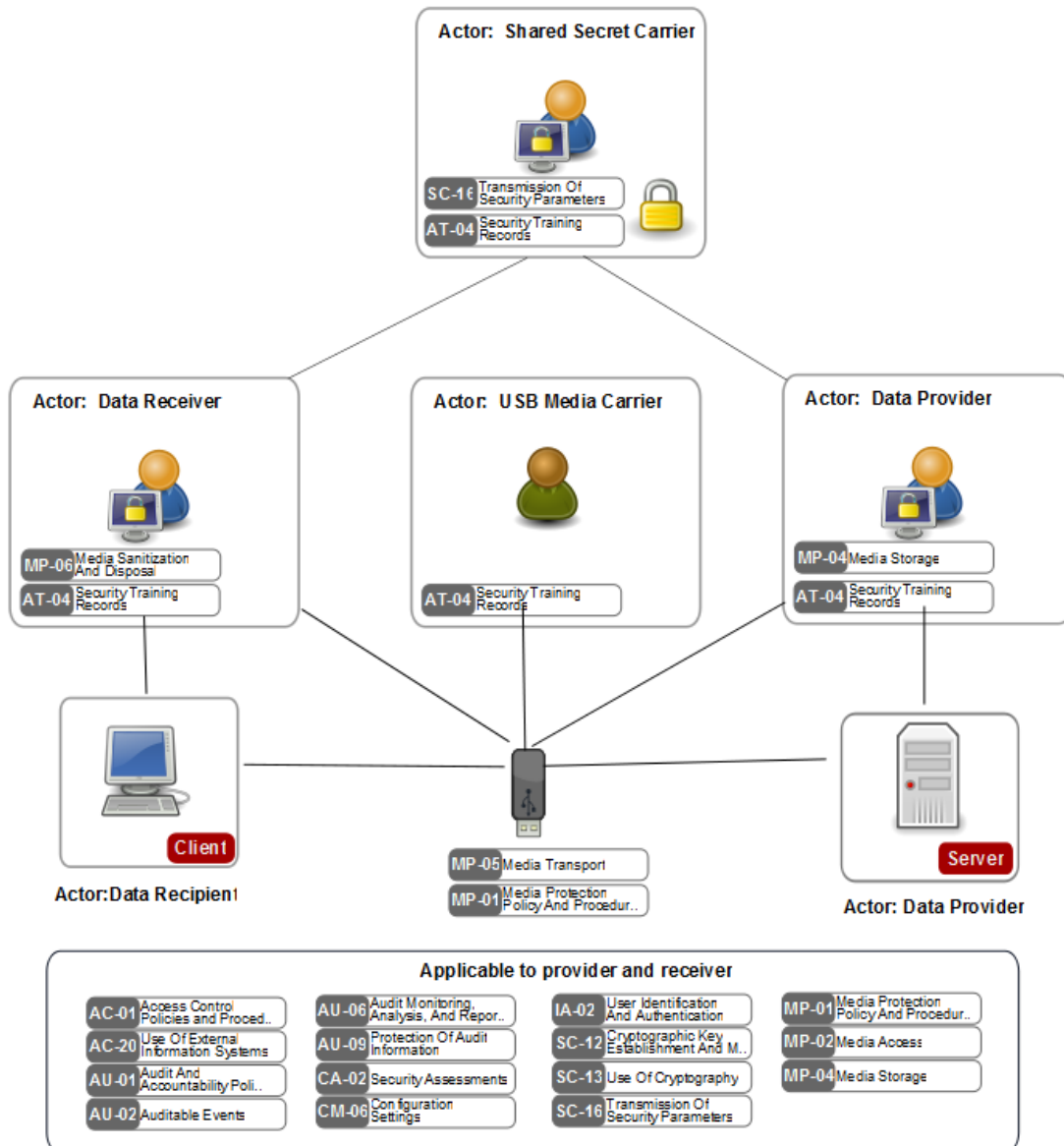
[AU-08 Time Stamps](#)

[AU-10 Non-Repudiation](#)

[AU-11 Audit Record Retention](#)

4.6 Removable Media / USB-Stick (Crypto)

Synopsis: Pattern for exchanging data via removable media by use of a secret-based (password) cryptographic protection control.



Description: A convenient and efficient way to exchange data is the use of removable media like USB sticks. To protect data from being accessed by unauthorized third-parties, encryption of the data is described. The process of encrypting data on the removable media is not transparent to the user. It requires the exchange of the secret (i.e. password) used. Awareness with users is therefore required to ensure proper selecting and handling of secrets. The exchange of the media may take place directly between provider and recipient or indirectly through a carrier.

Processes to consider:

- Media-crypto set-up process depending on removable media and crypto mechanisms involved
- Encryption of data stored on the removable media
- Exchange of removable media
- Exchange of secret
- Decryption of data

An initial set-up effort is required to configure the end-user computers to access the interfaces of the removable media, e.g. USB-ports, and to setup the crypto mechanisms. This effort is required from both sides.

Assumptions: Encryption and decryption mechanisms are provided on the provider's and the recipient's computers; read- and write-access to the removable media. End-to-end protection is required. State-of-the-Art crypto mechanisms are used.

Typical challenges: The exchange of the secret must not be combined with the exchange of the media if the media is transmitted by public postal service. The strength of the secret must be selected appropriately. Access to removable media is required. Respective protection mechanisms must be available at both places, potentially on different platforms (e.g. Linux and Windows).

Indications: Exchange of large amounts of data between two users.

Contra-indications: Disabled access to interfaces of removable media: In many companies, access to removable media is disabled. Proprietary, platform-specific protection mechanisms. Data exchange between many users.

Resistance against threats: Data exchange is protected on the removable media in an end-to-end manner by cryptographic means. A number of residual risks remain with this pattern:

- Confidentiality: Leakage of the secret together with the removable media. If the removable media is lost together with the secret, the protection relies on the availability of the encryption/decryption mechanisms with the holder of the media and the secret. It must not be considered secure anymore.
- Availability: Loss of the secret. If the secret is lost, e.g. forgotten, the data cannot be decrypted.
- Accidentally weak protection mechanisms: If errors in the algorithms or handling of the secret are implemented with the mechanisms, protection may be invalidated easily. The complexity resulting from implementing crypto-mechanisms correctly combined with the generally proprietary implementations increases the risk of weaknesses. While it is nearly impossible for a user to detect respective weaknesses, experts may easily access the plain information.
- Intentionally weak protection mechanisms: Algorithmic-backdoors. Beside maliciously implemented weaknesses in the crypto mechanisms, seeds, nonces and initialization vectors may be chosen by malicious intent. While for an outsider the weakness may not be revealed, an insider may easily access the plain information.

Implementation Variants:

- Crypto-mechanisms implemented as application to be run on the computer
- Crypto-mechanisms implemented as application to be run on the processor of the removable media
- Password- or certificate-based secret.
 - Various protection mechanisms for the secret exist
- Biometric secret

References:

- Multiple vendors do exist that provide respective solutions

Related patterns: other SIX patterns

Classification: Removable Media

Release: April 2011

Author(s): Lukas Ruf;
pattern was created based on the result of the SGRP Special Interest Group "Secure Information Exchange"

Reviewer(s): Walter Sprenger

Controls:

[AC-01 Access Control Policies and Procedures](#)

[AC-20 Use Of External Information Systems](#)

[AT-04 Security Training Records](#)

[AU-01 Audit And Accountability Policy](#)

[AU-02 Auditable Events](#)

[AU-06 Audit Monitoring, Analysis, And Reporting](#)

[AU-09 Protection Of Audit Information](#)

[CA-02 Security Assessments](#)

[CM-06 Configuration Settings](#)

[IA-02 User Identification And Authentication](#)

[SC-12 Cryptographic Key Establishment And Management](#)

[SC-13 Use Of Cryptography](#)

[SC-16 Transmission Of Security Parameters](#)

[MP-01 Media Protection Policy And Procedures](#)

[MP-02 Media Access](#)

[MP-04 Media Storage](#)

[MP-06 Media Sanitization And Disposal](#)

5 Conclusion

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.

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.

Technically it is possible to set up a secure data exchange solution. But 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.

6 Appendix

6.1 Reference / Links

OSA website – see <http://www.opensecurityarchitecture.org>

6.2 Legal Notice

All patterns were created based on the Special Interest Group (SIG) results of the SGRP and the Information Security Society Switzerland.

The views and recommendations presented in this document are solely the ones of the members of the Special Interest Group and do not represent official statements of the organisations SGRP and ISSS.

The two organisations do not accept any responsibility for the accuracy or intelligibility of the details given. All liability for the accuracy and completeness thereof or for any damage resulting from the use of the information contained in this whitepaper is expressly denied. Under no circumstances shall SGRP or ISSS be liable for any financial and/or consequential loss relating to this whitepaper.

6.3 Copyright



This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

