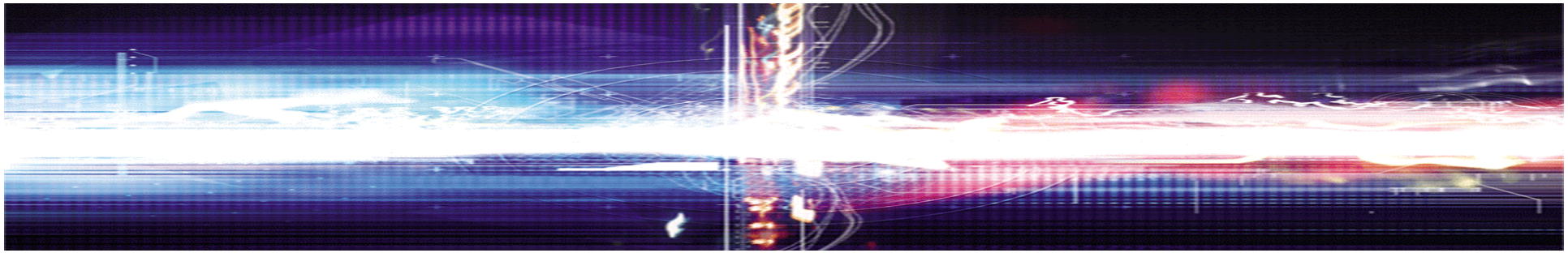


Sorgfalt im Umgang mit Identitätskennungen (fürs Zertifikat)

SIK/CSI

Schweizerische Informatikkonferenz
Conférence suisse sur l'informatique
Conferenza svizzera sull'informatica
Conferenza svizra d'informatica

Daniel Muster
daniel.muster@it-rm.ch
www.it-rm.ch
28. Nov. 2014

Einleitung

Begriff: Identitätskennung besteht aus ein oder mehreren Attributen, welche sich eindeutig auf eine Identität zurückführen oder zuordnen lassen!

Sorgfalt im Umgang mit Identitätskennungen bedeutet **nicht nur**:

- Sorgfalt im Umgang (Erfassen, Kopieren, Löschen) von digitalen Attributen
- Sorgfalt bei der Aufnahme der digitalen Attribute ins Zertifikat

Sondern auch:

- Sorgfalt in der Auswahl der Applikation, welche sensitive Daten bearbeitet.

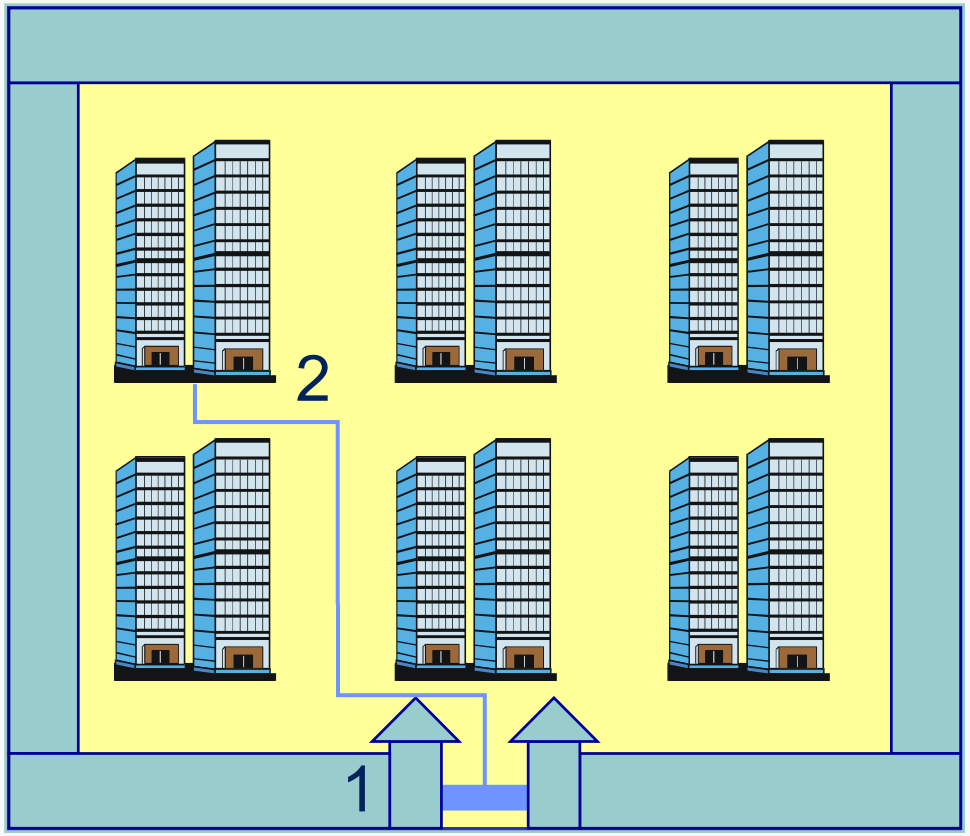
Einleitung

Inhalt des Vortrags:

- Problematik, Risiken
- Beispiel E-Mail, Web Applikation
- Lösungsansatz
- Fazit / Empfehlung
- Fragen

Problematik

Beispiel aus der physischen Welt:



Zugang zum Areal

Problematik

Beispiel aus der physischen Welt:

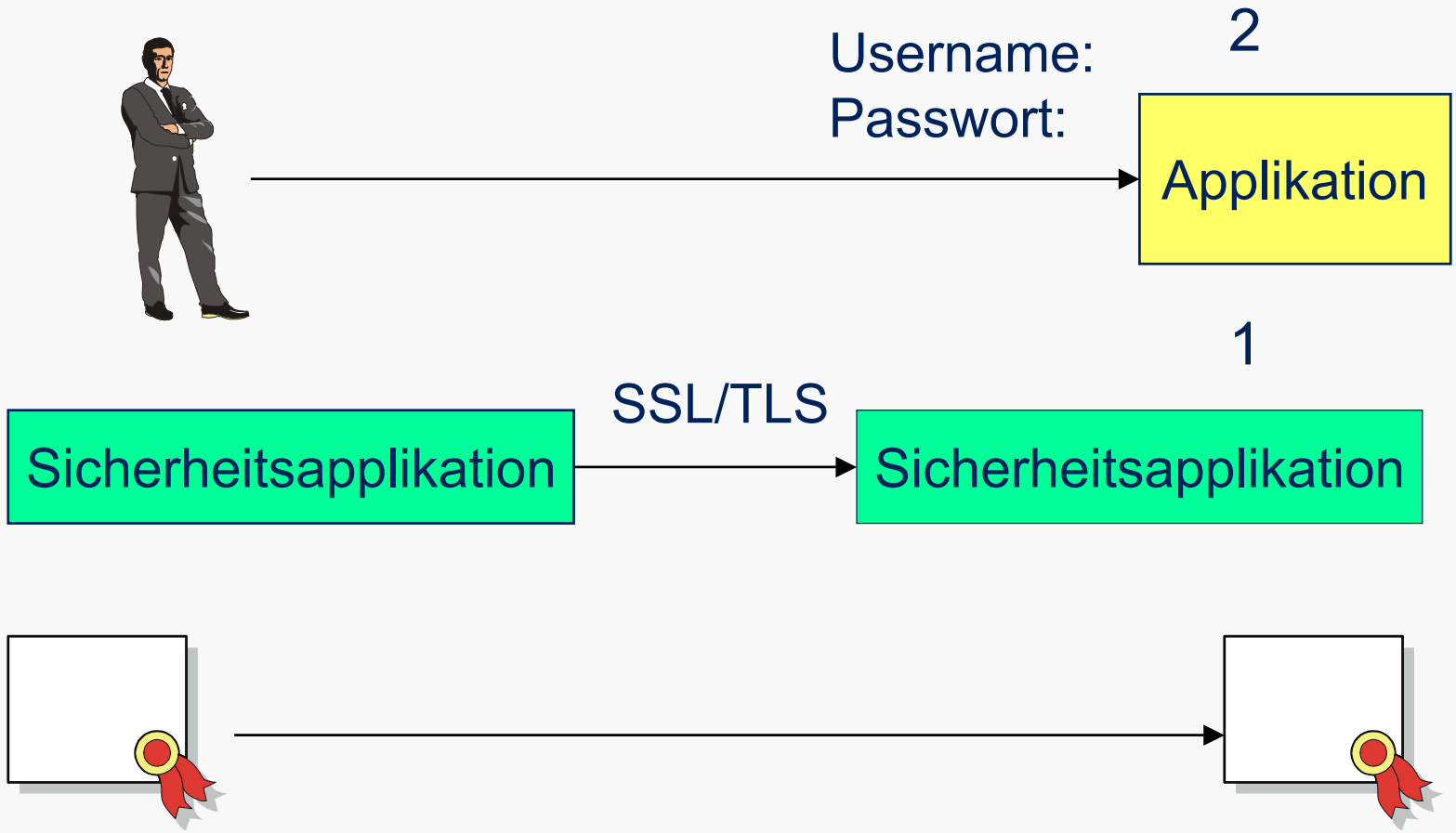
- Am Tor (1) wird gründlich die Identität überprüft.
- Am Eingang (2) muss er lediglich seine Visitenkarte vorweisen, um ins Gebäude zu kommen.

Risiko:

- Am Tor (1) mit ID XY identifiziert!
- Am Eingang (2) hat sich der Mitarbeiter mit der ID AB eines anderen Mitarbeiters ausgewiesen und somit seine Rechte unerlaubt erweitert.

Problematik

Beispiel aus der IT-Welt:



Problematik

Risiko:

- Auf Stufe SSL/TLS mit ID XY im Zertifikat authentisiert
- Bei der Applikation mit Username AB eines anderen Benutzers authentisiert und somit seine Rechte unerlaubt erweitert.

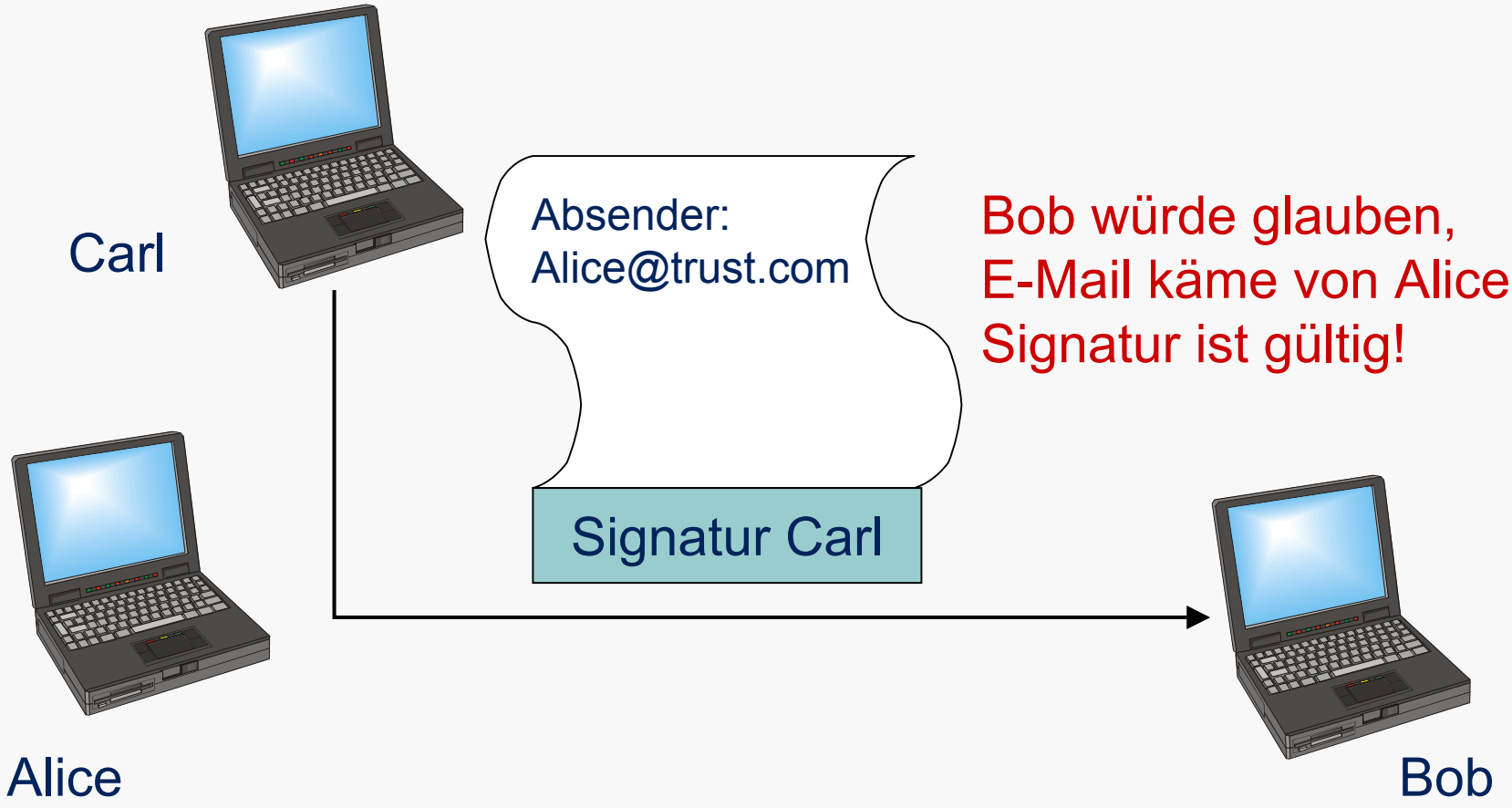
Lösungsansatz

E-Mail:

Wichtig: Bei der Signaturprüfung muss die angezeigte E-Mail Adresse mit der E-Mail Adresse im Zertifikat verglichen werden, welches für die Signaturprüfung verwendet wird!

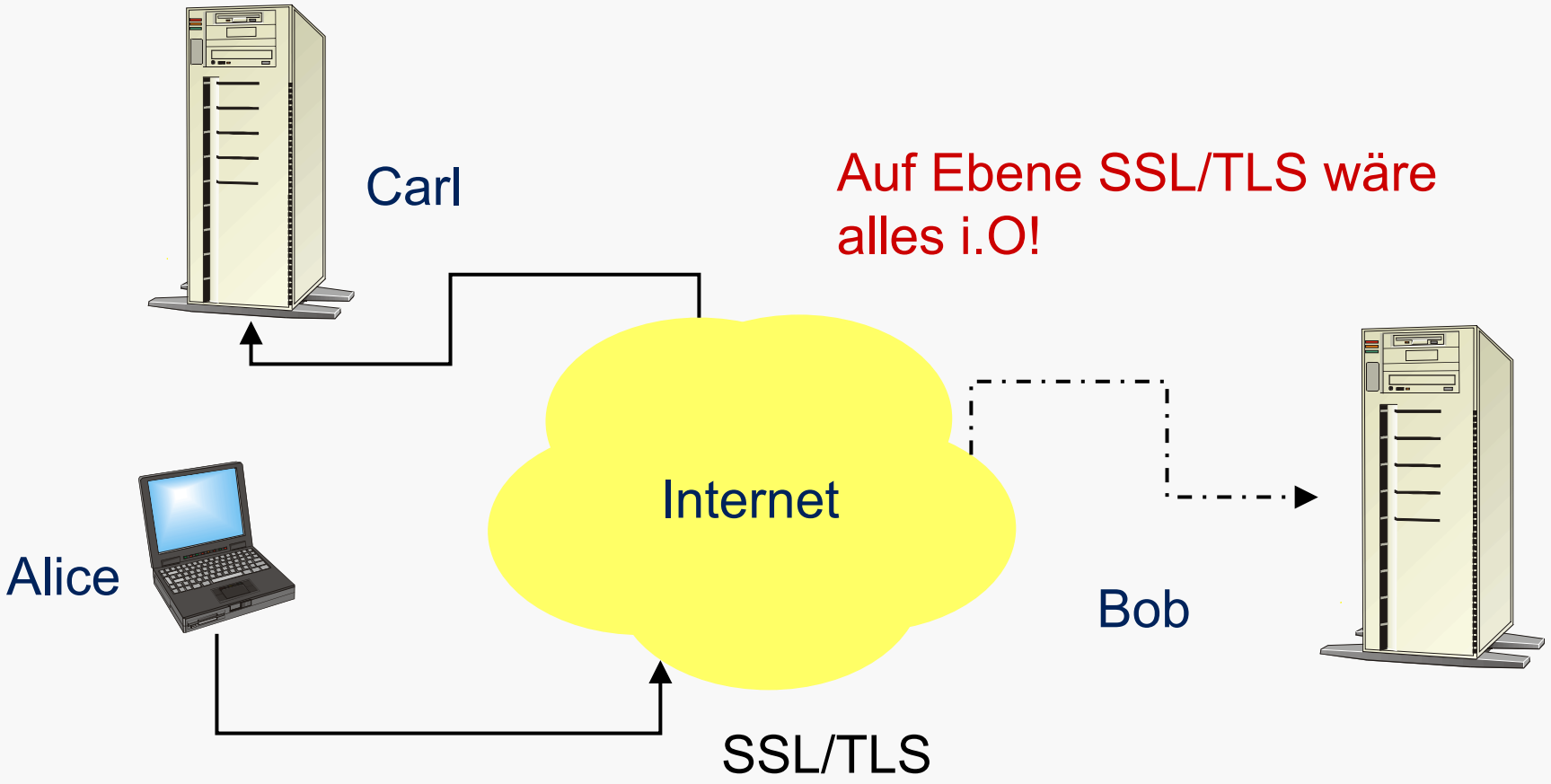
Lösungsansatz

E-Mail: Ansonsten besteht die Gefahr:



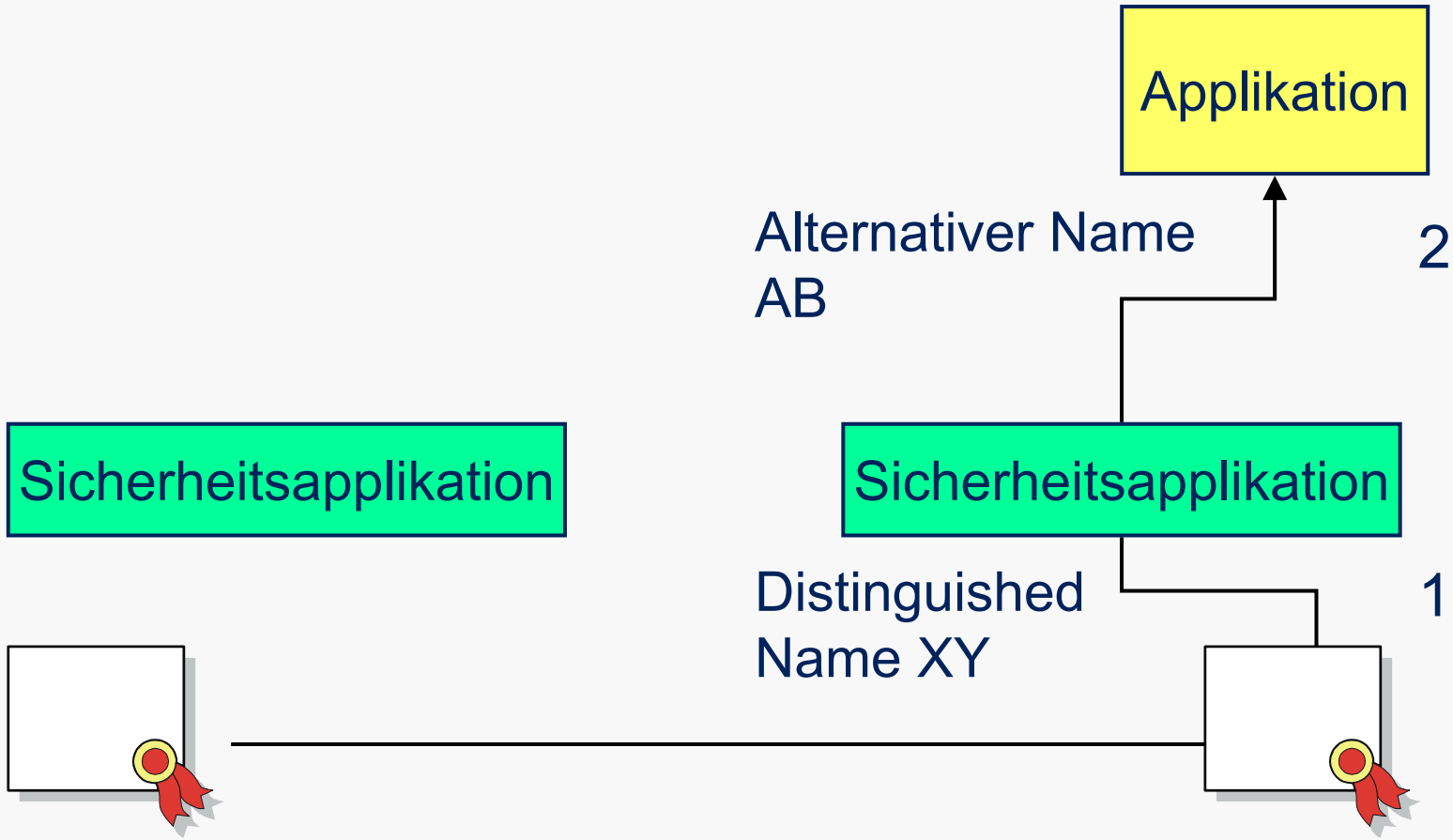
Lösungsansatz

SSL/TLS Client: Gefahr, wenn die URL im Zertifikat nicht mit der angewählten URL auf Übereinstimmung kontrolliert wird.



Lösungsansatz

SSL/TLS Server:



Lösungsansatz

SSL/TLS und Applikation:

- Auf Stufe SSL/TLS mit ID1 XY im Zertifikat findet eine Vorselektion statt.
- Nach erfolgter Authentisierung auf Stufe SSL/TLS wird ID2 AB (alternativer Name) im Zertifikat mit ID1 XY an die Applikation übergeben. Der Client vermag dies nicht zu beeinflussen.
- Aufgrund von ID2 AB wird dann die Authentisierung und Autorisierung in der Applikation vorgenommen!

Fazit / Empfehlung

Zwischen Applikation mit sensitiven Informationen und Sicherheitstechnologie sollte eine standardisierte oder definierte Schnittstelle zum Transfer von Identitätskennungen im Zertifikat vorhanden sein. Dies in beide Richtungen.

Wird eine Applikation mit schützenswerten Daten mit einer auf Zertifikat basierenden Authentisierung geschützt, dann sollte die Authentisierung und Autorisierung auf Ebene Applikation aufgrund von Attributen im Zertifikat vorgenommen werden.

=> Beim Verbindungsaufbau auf Client Seite: Angewählter Applikationsname muss nach erfolgreicher Authentisierung (SSL/TLS) des Servers mit dem entsprechenden Namen im Zertifikat verglichen werden!

Fazit / Empfehlung

=> Serverseite: Nach erfolgreicher Authentisierung des Clients auf Ebene Sicherheitstechnologie. Die Applikation sollte aufgrund der Identitätskennung im entsprechenden Zertifikat die Authentisierung und Autorisierung vornehmen. Wichtig: Der Client kann keinen Einfluss darauf nehmen!

=> Für schützenswerte Informationen Applikationen auswählen, deren Username ins Zertifikat aufgenommen werden kann.

=> RA: Bei der Aufnahme von Identitätskennungen sind alle sorgfältig auf Richtigkeit zu prüfen. Jedoch besonders die, welche Zugang zu sensitiven Informationen ermöglichen!

Fragen