Crypto-Agility: Identität und Authentifizierung

Sebastian Schulz | Sales Engineer EMEA

GlobalSign
GMO INTERNET GROUP

Präsentiert von:

Sebastian Schulz

Sales Engineer EMEA, GlobalSign

GlobalSign
GMO INTERNET GROUP

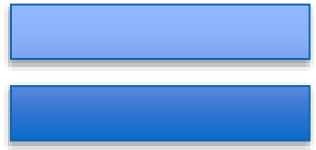
Agenda

- Zum Auffrischen: Wozu PKI und wie funktioniert das?
- Sinn und Zweck von Inventarisierung und Management von Zertifikaten
- Was genau ist “Crypto-Agility”?
- Warum Crypto-Agility größerem Schaden im Unternehmen vorkommen kann
- Wie GlobalSign mit Produkten und Partnerschaften zu Crypto-Agility beiträgt

Zum Auffrischen: Wozu PKI und wie funktioniert das?

Was sind Digitale Zertifikate?

- Wie ein „digitaler Pass“: Einzigartig und Fälschungssicher
- Ohne Public Key Infrastructure (PKI) keine digitalen Zertifikate



```
-----BEGIN CERTIFICATE-----
MIIDxzCCAq+gAwIBAgIIDq0DYy9e1dEwDQYJKoZIhvcNAQELBQAwVDELMAkGA1UE
BhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBUcnVzdCBTZXJ2aWNlczElMCMGA1UEAxMc
R29vZ2xlIEludGVybmV0IEF1dGhvcml0eSBHMzAeFw0xODEyMTkwODE2MDBaFw0x
OTAzMTMwODE2MDBaMGgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlh
MRYwFAYDVQQHDA1Nb3VudGFpbiBWaWV3MRMwEQYDVQQKDApHb29nbGUgTExDMRcw
FQYDVQQDDA53d3cuZ29vZ2xlLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BEv5RxuoqMukxsAtRd5D87z10pj0JZBvEw14GqwFtN979gZcgJeaUwbQ2w4VrQPe
FAnTd1SxThWor+P93J2t4MWjggFSMIIBTjATBgNVHSUEDDAKBggrBgEFBQcDATAO
BgNVHQ8BAf8EBAMCB4AwGQYDVR0RBBIwEIIOd3d3Lmdvb2dsZS5jb20waAYIKwYB
BQUHAQEEXDBaMC0GCCsGAQUFBzAChiFodHRwOi8vcGtpLmdvb2cvZ3NyMi9HVFNH
SUFHMy5jcnQwKQYIKwYBBQUHMAGGHWh0dHA6Ly9vY3NwLnBraS5nb29nL0dUU0dJ
QUczMB0GA1UdDgQWBBSgt0IIK7d/bpToVbC8gzOp6Fw/qjAMBgNVHRMBAf8EAjAA
MB8GA1UdIwQYMBaAFHfCuFCaZ3Z2sS3ChtCDoH6mfrpLMCEGA1UdIAQaMBgwDAYK
KwYBBAHWeQIFAzAIBgZngQwBAgIwMQYDVR0fBCowKDAmoCSgIoYgaHR0cDovL2Ny
bC5wa2kuZ29vZy9HVFNHSUFHMy5jcmwwDQYJKoZIhvcNAQELBQADggEBAKd6Yiud
9vFUkdoF3UnarCqa+DFK6HBz8PrPGUqxHiueeJPj/Y9MAyNGXhTXtnnhh/Ef+8Pd
zmfwDMJFF+r7+i8TKArGTK7Rl2FSQakTZejHWFFRpsnMrHGpzaABRGIZyGEZQAWs
JZqne6vu4e3g+ExhKbHIX3+W519vt5W0nXTNjM7UPTMqWfimmnRhcVb5IjJAhElo
d7Vt4Tybun81jegIeixvpVwSEX2MVg8v/iPdQtvBuDeKThtNcULWGKJLuD3TYlGN
ZjUcMIaFVTfEkZWL6bm2Ff77l7U9njFKPxToEorAAloJtepmiAVflECWYDAYyh0w
UfuSf04Rd2+/U5o=
-----END CERTIFICATE-----
```

PKI – ein Schweizer Taschenmesser

GlobalSign®

Key Usage

- Client Authentication
- Key Encipherment
- Digital Signature

Verifizierte Identität

- Einzelpersonen
- Abteilungen
- Firmen/Unternehmen

Wie funktioniert PKI genau?

- Basiert auf Asymmetrischer Kryptographie

Privater Schlüssel

Verschlüsselt Entschlüsselt

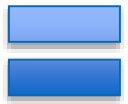
Daten/andere Schlüssel

- Eine strikte Hierarchie bestätigt Identität der Schlüsselinhaber
- Eine Registration Authority (RA) prüft diese Identität
- Eine Certificate Authority (CA) manifestiert das in Digitalen Zertifikaten

Entschlüsselt Verschlüsselt

Öffentlicher Schlüssel

Identität



Digitales Zertifikat

Sinn und Zweck von Inventarisierung und Management von Zertifikaten

Wie Zertifikate genutzt werden

GlobalSign®

Öffentliche Netzwerke

- SSL/TLS auf der Webseite
- S/MIME Verschlüsselung
- Digitale Signaturen

Interne Netzwerke

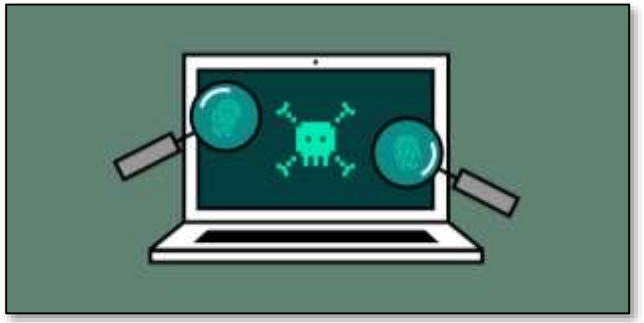
- Nutzer-Authentifizierung
- Geräte-Authentifizierung
- Datei-Verschlüsselung

Warum sollte man Zertifikate gut inventarisieren?

- Abgelaufene Zertifikate sind ungültig

- Nutzer und/oder Geräte werden ausgetauscht oder überfällig

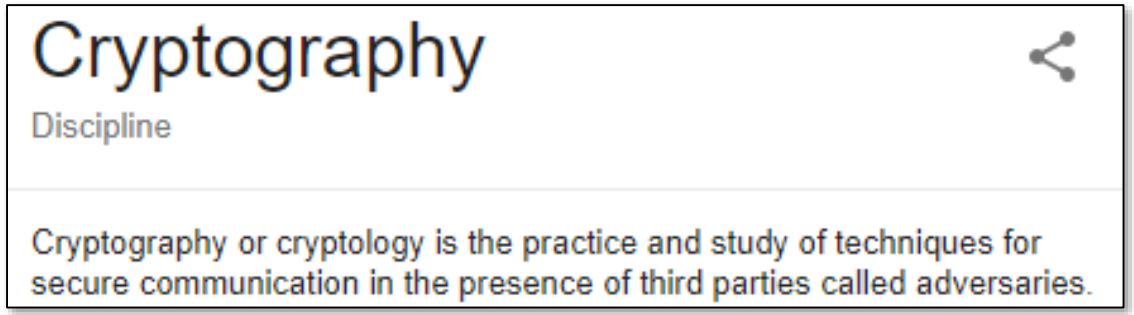
- Durch Hacking oder Phishing werden Schlüssel kompromittiert

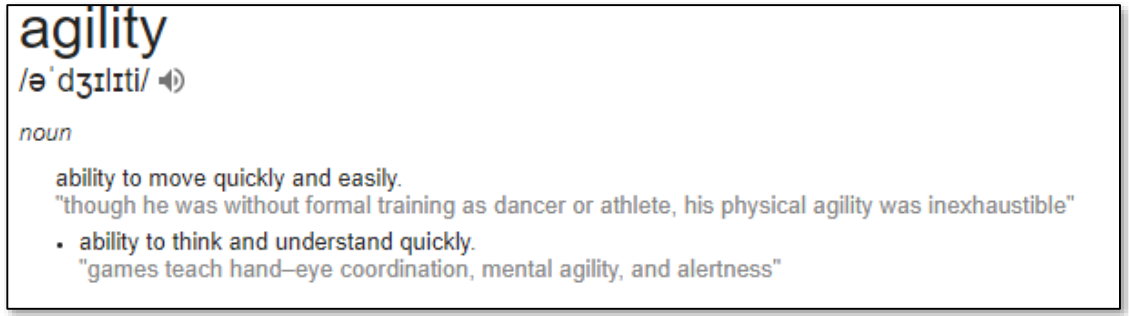


Was genau ist “Crypto-Agility”?

Aber was genau ist Crypto-Agility jetzt?

GlobalSign®





Crypto-Agility heißt bei der Implementation von Kryptographie in der IT spontan auf Änderungen im technischen oder juristischen Bereich reagieren zu können, seien sie noch so unvorhergesehen.

Wann und wo Crypto-Agility gefordert ist

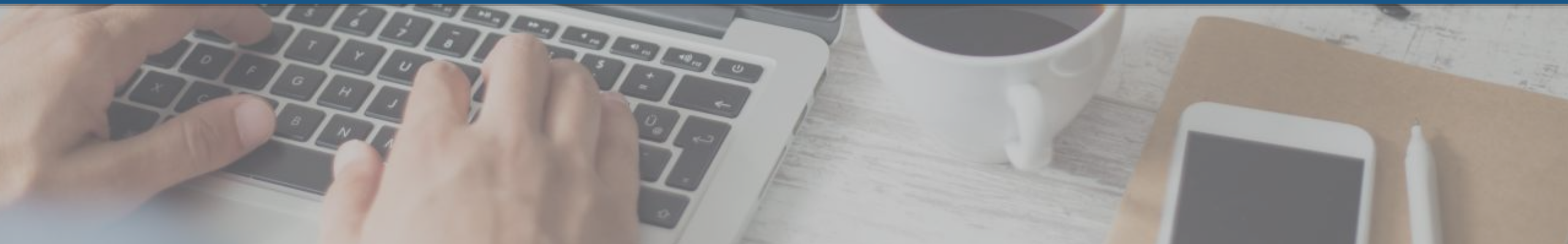
GlobalSign®

- Kryptographische Algorithmen können mit der Zeit veralten und angreifbar werden

- Gelegentlich tuen sich massive Sicherheitslücken in Protokollen auf

- Den Lebenszyklus von Zertifikaten zu managen ist so oder so unabdingbar

Warum Crypto-Agility größerem Schaden im Unternehmen vorkommen kann



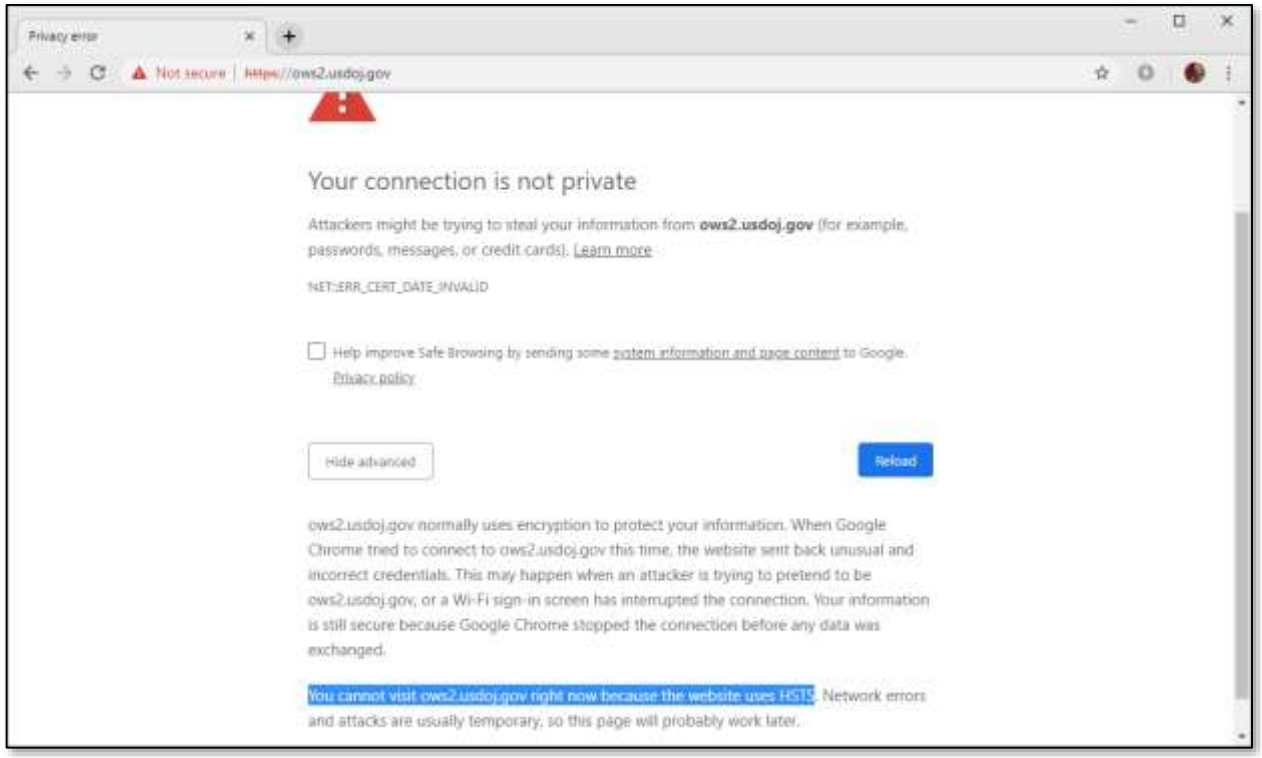
Die US-Regierung zum einen…

Website access disrupted during US government shutdown

11. Januar 2019 in BBC NEWS

US government shutdown leaves websites down

11. Januar 2019 in techradar.



…und O2 (Telefonica) zum Anderen

GlobalSign

Millions of smartphones in UK and Japan reportedly taken offline by Ericsson equipment issue

6. Dezember 2018 in THE VERGE

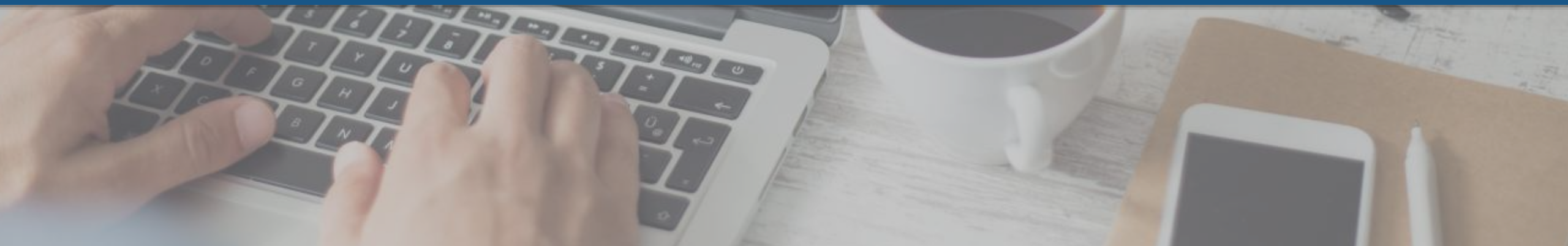
O2's All-Day Outage Caused Havoc in Ways Consumers Didn't Expect

8. Dezember 2018 in Bloomberg

*An initial root cause analysis indicates that the main issue was an **expired certificate** in the software versions installed with these customers.*

Pressemitteilung, 6.12.2018 15:50 von ERICSSON

Wie GlobalSign mit Produkten und Partnerschaften zu Crypto-Agility beiträgt



Crypto-Agility braucht Zertifikatsübersicht

Herausforderung?

Welche	Wo

Wessen	Was

Lösung!

Software

Cloud Services

GlobalSign GMO INTERNET GROUP

VENAFI

…und einigen Anderen!

Crypto-Agility braucht Zertifikatsmanagement

GlobalSign

Herausforderung?

Ausstellung

Verlängerung

Revozierung

Neuaustellung

Server

Endgerät

Lösung!

Server oder PC	Mobil
GlobalSign GMO INTERNET GROUP	Microsoft Intune
VENAFI	MobileIron
keytalk	airwatch

…und einigen Anderen!

Was GlobalSign bieten kann

Identität für Geräte und Maschinen

Web- und Server-Sicherheit

Nutzer- und Geräte-Authentifizierung

Managed PKI

Sichere Mobilgeräte

Sichere E-Mail

Digitale Unterschriften

“Public Key Infrastructure provides the framework that allows you to deploy security services based on encryption […]”

(PKI-Implementing and Managing E-Security **, Nash et al.**)

“Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on […] ”

(Interview mit „The Guardian“**, Edward Snowden**)

Weitere Fragen?

Sprechen Sie mit uns am Stand 611 in Halle 10.1!

Oder über soziale Medien:

www.globalsign.de

@globalsign_DE

GlobalSign

GlobalSign
GMO INTERNET GROUP