IWSz meets UCMD/UDM

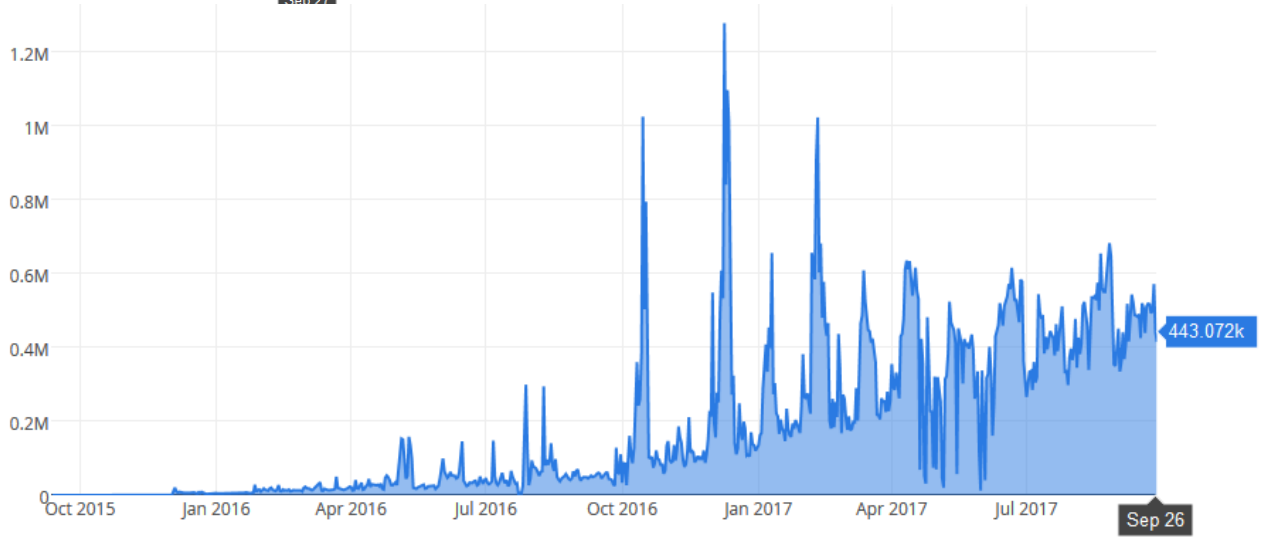
Enhanced Security through Certificates

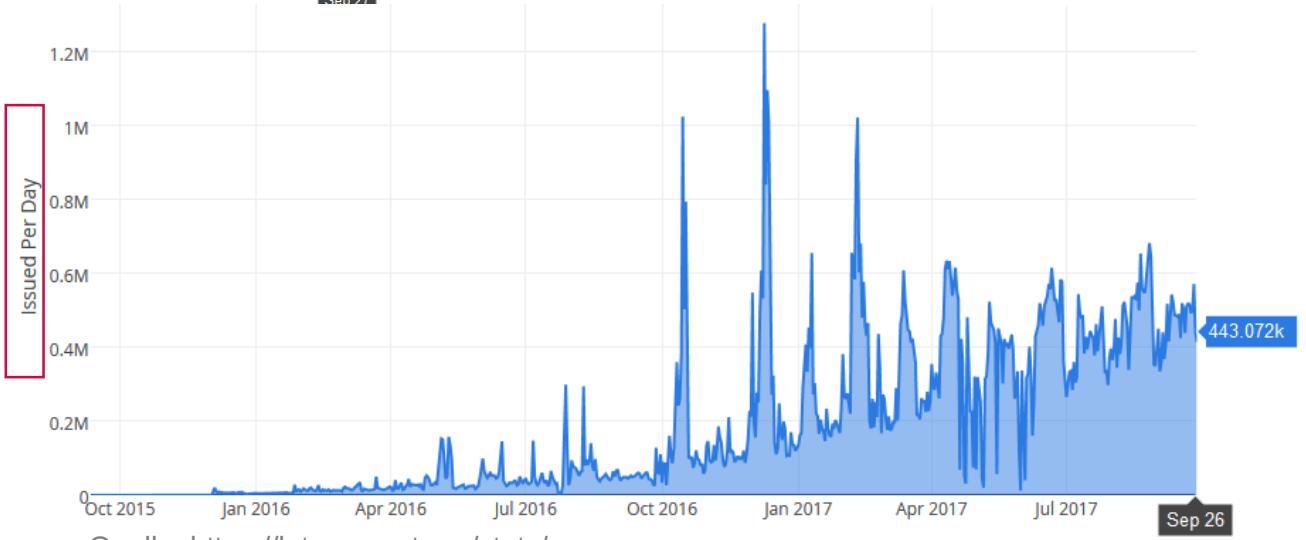
Donnerstag, 5. Oktober 2017

Lukas Essig

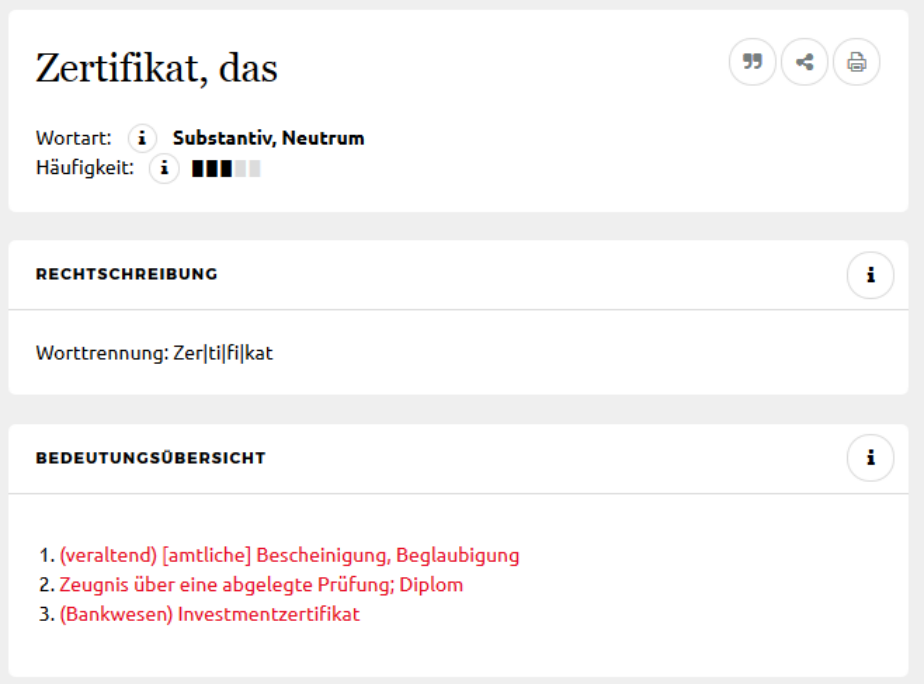
FIDUCIA GAD
ZUKUNFTSERFAHREN

IT-Partner der FinanzGruppe
Volksbanken Raiffeisenbanken





Quelle: https://letsencrypt.org/stats/



Zertifikat, das

Wortart: **Substantiv, Neutrum**
Häufigkeit:

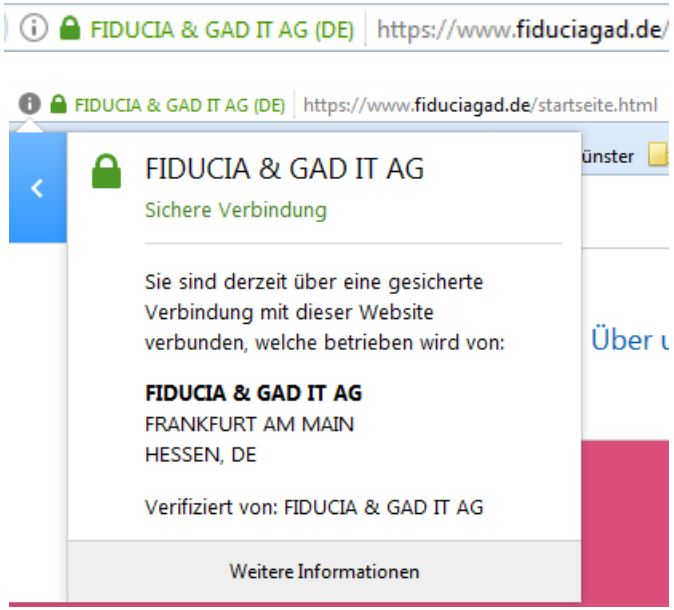
RECHTSCHREIBUNG

Worttrennung: Zer|ti|fi|kat

BEDEUTUNGSÜBERSICHT

1. (veraltend) [amtliche] Bescheinigung, Beglaubigung
2. Zeugnis über eine abgelegte Prüfung; Diplom
3. (Bankwesen) Investmentzertifikat

Quelle: http://www.duden.de/rechtschreibung/Zertifikat



Dieses Zertifikat wurde für die folgenden Verwendungen verifiziert:

SSL-Server-Zertifikat

Ausgestellt für

Allgemeiner Name (CN)	FIDUCIAGAD.DE
Organisation (O)	FIDUCIA & GAD IT AG
Organisationseinheit (OU)	VR-IDENT
Seriennummer	04:8E:69:5D:37:8E:CF:56:9B:99:1B:32

Ausgestellt von

Allgemeiner Name (CN)	VR IDENT EV SSL CA 2016
Organisation (O)	FIDUCIA & GAD IT AG
Organisationseinheit (OU)	VR IDENT

Gültigkeitsdauer

Beginnt mit	Donnerstag, 4. Mai 2017
Läuft ab am	Freitag, 2. August 2019

Fingerabdrücke

SHA-256-Fingerabdruck	98:61:6B:84:44:F1:EC:82:9D:94:63:A5:13:B6:61:56:82:F3:60:09:41:6E:8A:16:F5:F7:63:6A:64:B3:79:A3
SHA1-Fingerabdruck	D0:87:2C:BB:EB:A7:F3:92:95:35:E0:80:9A:D4:1A:10:F4:12:3D:9F

Zertifikatshierarchie

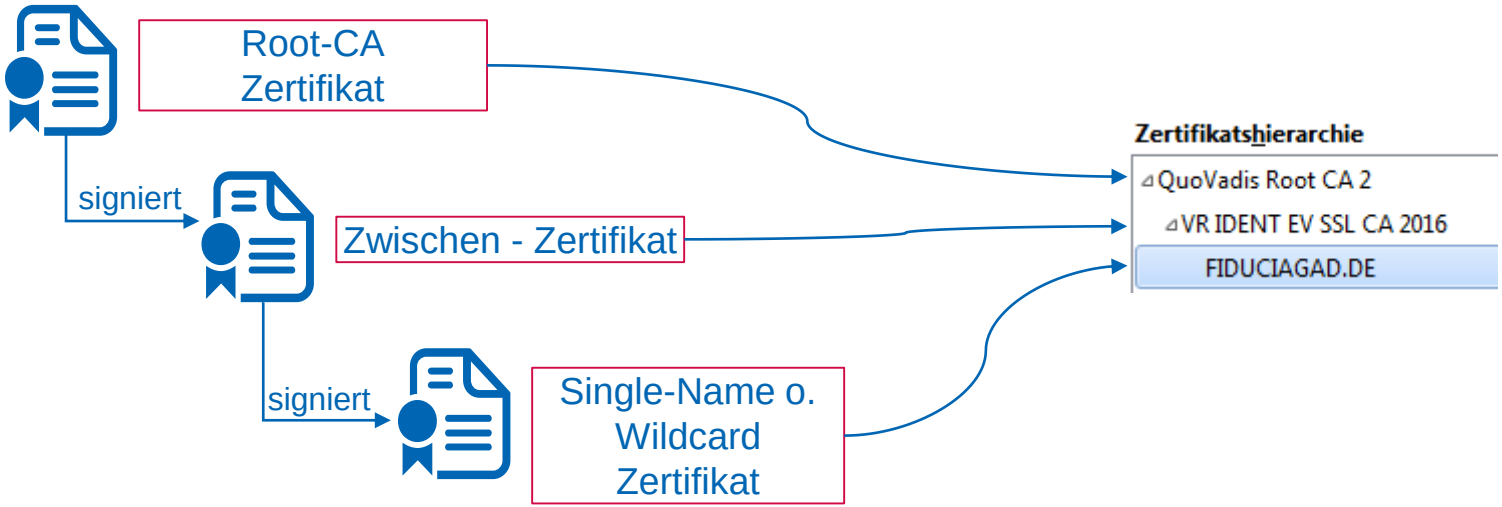
- QuoVadis Root CA 2
  - VR IDENT EV SSL CA 2016
    - FIDUCIAGAD.DE

Technische Details

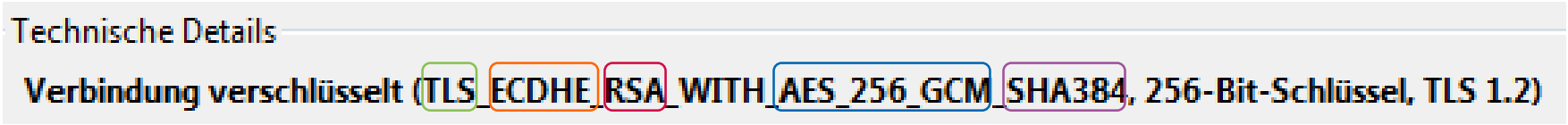
Verbindung verschlüsselt (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256-Bit-Schlüssel, TLS 1.2)

Cipher Suite

Chain of Trust



Cipher Suites



Protokoll
Schlüsselaustausch
Authentifizierung
Verschlüsselung und Key-Größe
Hashfunktion

Stonebranch Cipher-Suites

FIDUCIA GAD
ZUKUNFTSERFAHREN

Cipher Suite Name	Description
AES256-GCM-SHA384	256-bit AES encryption in Galois Counter Mode, SHA-2 384-bit message digest.
AES256-SHA	256-bit AES encryption with SHA-1 message digest.
AES128-GCM-SHA256	128-bit AES encryption in Galois Counter Mode, SHA-2 256-bit message digest.
AES128-SHA	128-bit AES encryption with SHA-1 message digest.
~~RC4-SHA~~	~~128-bit RC4 encryption with SHA-1 message digest.~~
~~RC4-MD5~~	~~128-bit RC4 encryption with MD5 message digest.~~
~~DES-CBC3-SHA~~	~~128-bit Triple-DES encryption with SHA-1 message digest.~~
~~DES-CBC-SHA~~	~~128-bit DES encryption with SHA-1 message digest.~~
~~NULL-SHA256~~	~~No encryption and SHA-2 256-bit message digest.~~
~~NULL-SHA~~	~~No encryption and SHA-1 message digest.~~
~~NULL-MD5~~	~~No encryption and MD5 message digest.~~
~~NULL-NULL~~	~~No encryption, no data authentication, SSL is not used, instead, Universal V2 Protocol~~ (**UNVv2**) is used.

https://www.stonebranch.com/confluence/display/UA64/SSL+Cipher+Suites+-+UCMD

Client
ucmd-manager

Verbindungsaufbau

Server
ubroker +
ucmd-server

Handshake

Client *alice*
ucmd-manager

Hallo, ist da jemand? ich möchte mit bob sprechen.

Ja hier ist bob. Das sagt auch trent. Aber wer bist du ?

Ich bin alice. Das sagt auch trent.

Schön. Dann lass uns unterhalten.
Aber über was entscheide ich!

trent bestätigt, dass bob bob ist

trent bestätigt, dass alice alice ist

Root-CA
trent

Server *bob*
ubroker +
ucmd-server

Was müssen wir tun?

1. Zertifikate beantragen
2. Nach Signierung einspielen,
    1. Server-Zertifikat(e) → in das Installationspaket
    2. Client-Zertifikat(e) → in das RACF
3. ucmd auf Client und Server entsprechend konfigurieren

Client ucmd-manager

```
HLQ.UNVCONF(UCMCFG00):
…
encrypt                     yes                          auf jeden Fall verschlüsseln
ctl_ssl_cipher_list         AES256-GCM-SHA384,AES256-SHA
data_ssl_cipher_list        AES256-GCM-SHA384,AES256-SHA  wie soll sich unterhalten werden
default_cipher              AES256-SHA
ssl_implementation          system                       IBM SSL oder OpenSSL
saf_key_ring                XCT1441/ALICE_KEYRING        Wo liegt mein Zertifikat + CA?
saf_key_ring_label          ALICE_UBROKER_CERT           Wie „heißt“ mein Zertifikat?
verify_host_name            bob.scheduling.zentral       mit wem möchte ich sprechen
…

XCT1441/ALICE_KEYRING:
Key ring owner              XCT1441

Certificate Label           Usage
trent-ROOT-CA               CERTAUTH
trent-SSL-CA                CERTAUTH
trent-SERVAUTH-CA           CERTAUTH
ALICE_UBROKER_CERT          PERSONAL
```

Server ubroker + ucmd-server

```
ubroker.conf:
…
ctl_ssl_cipher_list     "AES256-GCM-SHA384,AES256-SHA"
certificate             /opt/universal/data/bob.scheduling.zentral.crt
private_key             /opt/universal/data/bob.scheduling.zentral.key
private_key_password    *strenggeheim*
ca_certificates         /opt/universal/data/trents_ca.crt

ucmds.conf:
…
encrypt                 yes
authenticate            yes
encrypt_control_session yes
data_ssl_cipher_list    "AES256-GCM-SHA384,AES256-SHA"
…
```

Server uacl.conf

```
uacl.conf:
cert_map id=alice,subject="/C=DE/ST=BADEN-
WUERTTEMBERG/L=KARLSRUHE/O=FIDUCIA?&?GAD?IT?AG/OU=SchedulingZentral/CN=ALICE_UBROKER_CERT"
cert_map id=dave,subject="/C=DE/ST=Baden-
Wuerttemberg/L=Karlsruhe/O=Fiducia?&?GAD?IT?AG/OU=FiletransferZentral/CN=udm.filetransfer.zentral"

# ucmd_cert_access certid,local_user,access,auth
ucmd_access ALL,*,*,deny,auth                    alle ohne Zertifikat abweisen
ucmd_cert_access alice,*,allow,auth              Darf alice überhaupt mit mir sprechen?
ucmd_cert_access dave,*,allow,auth               Darf dave überhaupt mit mir sprechen?
ucmd_cert_access *,*,deny,auth                   Der Rest mit Zertifikat darf nichts

# ucmd_cert_request certid,local_user,req_type,req_name,access,auth
ucmd_request ALL,*,*,*,*,deny,auth               alle ohne Zertifikat (nochmals) abweisen
ucmd_cert_request alice,*,*,*,allow,auth         Was darf alice mir befehlen?
ucmd_cert_request dave,*,shell,?*,allow,auth     Was darf dave mir befehlen?
ucmd_cert_request *,*,*,*,deny,auth              Der Rest mit Zertifikat darf (nochmal) nichts
…
```

Positiv-Test

```
UNV2578I Universal Command Manager component 1504605360 registered with local Broker alice‘
UNV0555A Local Broker options:
UNV2571A    System identifier: alice
UNV0562A    Default options:
UNV0563A        Codepage: dd:UNVNLS(IBM1141)
UNV0564A        Comp: yes,zlib, Encrypt: yes, Auth: yes, FT: yes
UNV2557A    SSL implementation: system
UNV2529A    Control session SSL cipher list: AES256-GCM-SHA384:AES256-SHA
UNV2530A    Data session SSL cipher list: AES256-GCM-SHA384:AES256-SHA
UNV2531A    Default SSL cipher: AES256-SHA
UNV2534A    Verify Broker certificate host: bob.scheduling.zentral
UNV2560I Using a command ID of dd:SCRIPTIN
UNV0522I Connecting to broker at 10.8.0.226, 6030.
UNV0548I Universal Command Server component 1504189774 started.
UNV2510I cntl   : Protocol=TLSV1.2, Kx=RSA, Au=RSA, Enc=AES(128), Mac=SHA384
UNV2511I cntl   : Port=10916, Compression=None, NFT=yes, Mode=txt,ucs
UNV2510I stdin  : Protocol=TLSV1.2, Kx=RSA, Au=RSA, Enc=AES(128), Mac=SHA384
UNV2511I stdin  : Port=10918, Compression=zlib, NFT=yes, Mode=txt,dir
UNV2510I stdout : Protocol=TLSV1.2, Kx=RSA, Au=RSA, Enc=AES(128), Mac=SHA384
UNV2511I stdout : Port=10919, Compression=zlib, NFT=yes, Mode=txt,dir
UNV2510I stderr : Protocol=TLSV1.2, Kx=RSA, Au=RSA, Enc=AES(128), Mac=SHA384
UNV2511I stderr : Port=10920, Compression=zlib, NFT=yes, Mode=txt,dir
UNV0523I Process 11181 started at remote time 14:35:45 10/02/17.
UNV2512I stdin  : Network Count=0            File Count=0
UNV2512I stdout : Network Count=92           File Count=72
UNV2512I stderr : Network Count=0            File Count=0
UNV0524I Process 11181 ended with exit code 0 at remote time 14:35:45 10/02/17.
```

Fragen? Fragen!

Contact me!

Lukas Essig
Fiducia & GAD IT AG
Fiduciastraße 20 | 76227 Karlsruhe

+49 721 4004 6377

mailto:lukas.essig@fiduciagad.de

FIDUCIA GAD
ZUKUNFTSERFAHREN

IT-Partner der FinanzGruppe
Volksbanken Raiffeisenbanken