Security Advisory Report - OBSO-1511-02-A

Appendix: Default Phone Certificates for OpenStage and OpenScape Desk Phone IP - web based management interface (https/443)

Creation Date: 2015-11-30
Last Update: 2015-11-30

Summary

This appendix to Unify Security Advisory OBSO-1511-02 includes the certificates (incl. their private keys) as used by default on all OpenStage / OpenScape Desk Phone IP phones provided by Unify.

Important Note: It is usually **not** advised to publish private keys associated with any X.509 certificate!
This document however emphasizes that these particular private keys are treated as "compromised by design". Therefore, the associated certificate should never be considered trusted.

For more information refer to Unify Security Advisory OBSO-1511-02 at https://www.unify.com/security/advisories

Vulnerability Details

Certificate #1:

- Valid since: 2013-10-15
- Reason: Initial creation due to Company Rebrand (Siemens Enterprise Communications -> Unify)
- Fingerprint: 2a370dcbc318c5d6178a7f7bd00530ca99276f3e
- subject=/C= /O=Unify GmbH & Co. KG/CN=Default Certificate for OpenStage/Desk Phone IP - please update
- issuer=/C= /O=Unify GmbH & Co. KG/CN=Root CA Certificate for OpenStage/Desk Phone IP - please update

```
-----BEGIN CERTIFICATE-----
MIIC3DCCAkWgAwIBAgIJAOS1LKZhSYivMA0GCSqGSIb3DQEBBAUAMHUxCzAJBgNV
BAYTAiAgMRwwGgYDVQQKFBNVbmlmeSBHbWJIICYgQ28uIEtHMUgwRgYDVQQDEz9S
b290IENBIENlcnRpZmljYXRlIGZvciBPcGVuU3RhZ2UvRGVzayBQaG9uZSBJUCAt
IHBsZWFzZSB1cGRhdGUwHhcNMTMxMDE1MTUwMzI2WhcNMzMxMDE1MTUwMzI2WjB1
MQswCQYDVQQGEwIgIDEcMBoGA1UEChQTVW5pZnkgR21iSCAmIENvLiBLRzFIMEYG
A1UEAxM/RGVmYXVsdCBDZXJ0aWZpY2F0ZSBmb3IgT3BlblN0YWdlL0Rlc2sgUGhv
bmUgSVAgLSBwbGVhc2UgdXBkYXRlMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQC8tRXUsiJG2ESfB5JdSw9dOBNFvchX8LQm3x5oLNQUqwK9pjChx9vn/vd3pokt
9vmWK/mWDmrYLMj9HTisIF2rfrA3XtrodWOvbpsaYiiXGy45lUNvgRHrtRKghKXw
jy7Mc3HuZear6FKWy75gdizBra1NjaHK9XH1ORKFZJaBlwIDAQABo3QwcjAdBgNV
HSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEQYJYIZIAYb4QgEBBAQDAgTwMB0G
A1UdDgQWBBS89QnF8MpRntvFW8eXN7x3vUS0WjAfBgNVHSMEGDAWgBQyiqTHDu4d
y+nlJlVc4f1M1X7vQDANBgkqhkiG9w0BAQQFAAOBgQCFUe8KgR//cm6KJF8P5fC5
z8Wya/6XkJxz0kGZX3Aq1WcyEBUv1duToFYgurstBeXeMZfae3nSTnS6BliIHCDT
doC0MlEgdKuaaSbEfQ3R0P/kHHA30zY0ijPhgBfrGCun682UF7TlL822BazV7oXY
n9wfFxsHlv0LRL9vBSfNug==
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC8tRXUsiJG2ESfB5JdSw9dOBNFvchX8LQm3x5oLNQUqwK9pjCh
x9vn/vd3pokt9vmWK/mWDmrYLMj9HTisIF2rfrA3XtrodWOvbpsaYiiXGy45lUNv
gRHrtRKghKXwjy7Mc3HuZear6FKWy75gdizBra1NjaHK9XH1ORKFZJaBlwIDAQAB
AoGBAIU1s5Z0tPubuT0lxC11SgA9EGW/5cgmU5XJFRbm5kM8wO+NfHEHu3WWp6xf
9CBtYpyeqE5EGSpG2w7KbPIc2uF4uvE8O0sUkWEWXRpfsw8g33qdSS+amoUhwo5J
QfwmCTvxnab6g9pKDXxAlyqbjBzcncuQyc0prm4xWgfj8AkxAkEA65UXf9qO6e7o
PCAJZHuun348SNSe7g8ioUQIqFoTINFU7qqjxGKJAXbL5YAXe+C8y8CvuklIE3Yz
3U9sgGa+GQJBAM0P+A/Cpg2DzylTvwdUQW+SMxHVV23Df9bBujVf2ZoM9BG+Padc
TRn09pB/h8kSX549S4slqG5Sohm3s8bD0y8CQG1BdeaLvB/t9rJ7wR9i5Pd/GgJE
6XhKeKsF3GYHcDuWGaeeZ9kaQaP2LlW/dCS1c5mjQVxJxC2Scjc/MHjULXECQB38
Gsq7LKrHPlCNtV4t/M+CskMGTh13u8a8Vy0c0eXLxRifF8bUIVYNUsx4SXOmYyLx
VY2IOSPAo4FdMkV7NvMCQFvGVR1IrHTab0Iwvu6orRNeeCtIfYE7Kw2wCxLZe+R/
cYWox6Ul7yT7YoRNy9seuZ4iMiMhiIK9hSJsB9bmpe0=
-----END RSA PRIVATE KEY-----
```

Certificate #2:

- Valid since: 2014-11-07
- Reason: Change signature algorithm from md5RSA to sha1RSA (to align with minimum modern browser requirements as a "helper" for those who don't want to configure customized X.509 certificates)
- Fingerprint: f215a701842b8898cf4dd7db978af1de0ef7551d
- subject=/O=Unify GmbH & Co. KG/CN=Default Certificate for OpenStage Desk Phone IP - please update
- issuer=/O=Unify GmbH & Co. KG/CN=RootCA Certificate for OpenStage/Desk Phone IP - please update

```
-----BEGIN CERTIFICATE-----
MIICwTCCAiqgAwIBAgIJAMl9FgwbpqTrMA0GCSqGSIb3DQEBBQUAMGcxHDAaBgNV
BAoME1VuaWZ5IEdtYkggJiBDby4gS0cxRzBFBgNVBAMMPlJvb3RDQSBDZXJ0aWZp
Y220ZSBmb3IgT3BlblN0YWdlL0Rlc2sgUGhvbmUgSVAgLSBwbGVhc2UgdXBkYXRl
MB4XDTE0MTEwNzEwNDAwMVoXDTM4MDExODEwNDAwMVowaDEcMBoGA1UECgwTVW5p
ZnkgR21iSCAmIENvLiBLRzFIMEYGA1UEAww/RGVmYXVsdCBDZXJ0aWZpY2F0ZSBm
b3IgT3BlblN0YWdlIERlc2sgUGhvbmUgSVAgLSBwbGVhc2UgdXBkYXRlMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC0D324XQpfe9I/W6L8XaOVnO+myLXL7PRj
jLqsfOjHjmt0eoew6flAVJz16fippT/0DFZLFdxI6TyrNY1vbWoE+HrkSotllVEf
wvT2Kse0T8037u9xuAl0xsK0FAV/aJ+JIf1APf6tjK9YVeVQXcFzrbWGDirVSj1e
5mGZJX9p1wIDAQABo3QwcjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw
EQYJYIZIAYb4QgEBBAQDAgTwMB0GA1UdDgQWBBTSI3uaEeZSq+mpdz+3dBF7Mkfp
9zAfBgNVHSMEGDAWgBQksm3PgBF/zK5Yn/inQsJd1kyYtTANBgkqhkiG9w0BAQUF
AAOBgQBUlqCg+8+tm0GHf/emoei1JgZGBtbeaReIijLg1xoohAzCv7RP0/rZimo1
4Kag/mJI7x/NMS/5Spc7jfcElGiplkxjVsglGsjmtd1gkFXs7eWY38aQSCxb3Dcw
QTsiOAw4LZDOhIbClnuR2sEDpiLPKuFPZZHBfTb9rYwCMOtoDw==
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQC0D324XQpfe9I/W6L8XaOVnO+myLXL7PRjjLqsfOjHjmt0eoew
6flAVJz16fippT/0DFZLFdxI6TyrNY1vbWoE+HrkSotllVEfwvT2Kse0T8037u9x
uAl0xsK0FAV/aJ+JIf1APf6tjK9YVeVQXcFzrbWGDirVSj1e5mGZJX9p1wIDAQAB
AoGAKzhosf9LRR4gmmqxlagYYwo3kC4vTRLEmryl9k9JRNVPv7bFqVaQKLvmrTSL
JpVu43Kup/lIVgv+Lw58s5lsz/t7GJftxk7/m1HzSXx0JnsBow6HPAlHv1wPbLjk
YlaC58bzour8t4o9wwWHFQxdFMVHds/h1u1x0BUqUIsfvbkCQQDfKFRwi3ZTHrAO
h6kYuXWwmKp6B1UnFDHxTocqyIzQUpdv1xd76+oBWqg1TeZVdiRLJHkAnmmqMCtD
PM2zFXilAkEAzo9wtBewsLZgpISMhogeYZ/DE1NQGKrIXKA3IDE6FigYk2rzKLNX
2KRLTsIKqW7qH/R3BV5aWrKdQNg/mcqTywJAcBBhrw7qAb3EbdeEfE0OI/vWiGdM
RM6oceScjkieJjODpv9d5LZJEhsDo5kWFU651R5gwYXLzFJaN26+YbNjnQJASNqo
yqxMYpeA0KX7lnuuE4qw2EEbUAf0cU8FAnK6ZRQxTtV6/BD9W+jesuGXtxjqtOiZ
jigwQCsdccCT9h9QLwJAY0fw7KtCS0P+yyQH8ywhpdLiX5cTw1wK19wb+bwMcucL
mGIjkghVFdWzFUNzKDZI7Pq9WB7o9RYpwmuyOKjoZQ==
-----END RSA PRIVATE KEY-----
```

Certificate #3:

- Valid since: 2015-09-07
- Reason: LE-Split (new name: Unify Software and Solutions)
- Fingerprint: 0a02d7f037ce46fb6f4afa8dae216a909c85f054
- subject=subject=/O=Unify Software and Solutions GmbH & Co. KG/CN=Default Certificate for OpenStage and Desk Phone - please update
- issuer=/O=Unify Software and Solutions GmbH & Co. KG/CN=Root CA Certificate for OpenStage and Desk Phone - please update

```
-----BEGIN CERTIFICATE-----
MIIC9DCCAl2gAwIBAgIJAL3Bj6ck+xDiMA0GCSqGSIb3DQEBBQUAMIGAMTMwMQYD
VQQKFCpVbmlmeSBTb2Z0d2FyZSBhbmQgU29sdXRpb25zIEdtYkggJiBDby4gS0cx
STBHBgNVBAMTQFJvb3QgQ0EgQ2VydGlmaWNhdGUgZm9yIE9wZW5TdGFnZSBhbmQg
RGVzayBQaG9uZSAtIHBsZWFzZSB1cGRhdGUwHhcNMTUwOTA3MTI1MTE4WhcNMzgx
MTE4MTI1MTE4WjCBgDEzMDEGA1UEChQqVW5pZnkgU29mdHdhcmUgYW5kIFNvbHV0
aW9ucyBHbWJIICYgQ28uIEtHMUkwRwYDVQQDE0BEZWZhdWx0IENlcnRpZmljYXRl
IGZvciBPcGVuU3RhZ2UgYW5kIERlc2sgUGhvbmUgLSBwbGVhc2UgdXBkYXRlMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/WmrpmCSOniWf6UbUEL3bcDBy3gnL
TiJ3bH+fse66d8Zd1CRj4A/Bbeic4mEvJ98jvDAevF19zD7Z+eixekAluuSlgPfv
KU/pbfeRI5ZHvqIlIoKn2TDMI/oOjFl1Ybz+u7eH5gYPXDipHiwBP4js+CrZgS4w
NbmO0s1s+YTtGQIDAQABo3QwcjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUH
AwIwEQYJYIZIAYb4QgEBBAQDAgTwMB0GA1UdDgQWBBQkoUmVPEAmqYXiMbdBehsK
XNPo3jAfBgNVHSMEGDAWgBQJ//4Tq6xNiGynoYuYaTowAn7PDzANBgkqhkiG9w0B
AQUFAAOBgQCrSF3RsutrylXy1Nm2VlUeYBiF9ifSHbbGO29x7f0jJdDBGCOETE0v
M6sTxjfqPlTNySkR55A5vz8+ad3O7Y8ovMttkcxLEzanr5TxxApzi0OuISxfNt2M
QqbnohiN2VxVEW4uWcabyo4mx5srgVvm/cYBVDKex9OOkOXMrmSoRw==
-----END CERTIFICATE-----
```

```
-----BEGIN RSA PRIVATE KEY-----
MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBAL9aaumYJI6eJZ/p
RtQQvdtwMHLeCctOIndsf5+x7rp3xl3UJGPgD8Ft6JziYS8n3yO8MB68XX3MPtn5
6LF6QCW65KWA9+8pT+lt95Ejlke+oiUigqfZMMwj+g6MWXVhvP67t4fmBg9cOKke
LAE/iOz4KtmBLjA1uY7SzWz5hO0ZAgMBAAECgYBrHWQnqwEbzK9nGqCJaW29/slA
I8b7xZtJmrS+Yk4ul4m1UGGmfvCS6MGDwL2CNiGU0W1mZy82kjTEtD5ryvFItHn3
DvNlMafztTAbRnfNsc8i0eI6uPjPO5rx8DIXCwMqpiXTFHSTmrB5epWsv6uyVh6u
CjqbSwMrnuvmf1XnAQJBAPWTmiANvHphxqBsvR4eDaXOp5xHqXwwri1sxZRKi5LS
PXaiz3iebagDTxCj9sVbzNYJrSYJlTATemUQd2lIL4kCQQDHeaHuuK4a9TA0+Tur
rm6W2HRR7c+oPfS0l+GLhSRqvMV5uICyr6jazAXHB7tHqldYe3D8la7CR0/wBff0
jV0RAkEAmusNPJFNyCpsQgG24Av3chTG2ai/e2++QTuv/Jd2Kx3j1jZpCV9wL6A+
vXGiF+iMdK3QBAHhkl2HRcA4hDsceQJBAJfXV9OfEzEEGRkJ60kpc5cx14GSE/NO
jhp2TsLkq67wWSXps1XRbyh2C6PQl9faq7h35q7uxeOvYwMjl/a5MPECQBiiyawY
pPb8Uyb1ocFQmzmAbSh1lRNQiWIdk0Z1Zf0mnnLXOIK4EBhbQFSR/YiPDF8jPHta
aiNmLcaHEK8nSC0=
-----END RSA PRIVATE KEY-----
```

Affected Products

See OBSO-1511-02.

Recommended Actions

When accessing a phone's web based management interface using https://<dnsname-or-ip-address-of-the-phone>: If the browser alerts you that one of these certificates are used, then the phone has not yet been configured with a suitable TLS server certificate to establish an encrypted and authenticated session.

In such situations, do not logon to the phone if there is a risk that untrusted 3rd parties may be able to intercept the communication between your browser and the device. This especially applies when you connect to the phone via the Internet.
Although your session would still be encrypted, the phone's authenticity could not be validated by your browser, so it could also be a 3rd party user or system who pretends to be the phone; therefore you should treat the https session as if it were a http session only.

References

- Unify Security Advisory OBSO-1511-02

Revision History

2015-11-30: Initial release

Advisory ID: OBSO-1511-02-A (a=126), status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer
OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com