WISeKey CertifyID Qualified Services CA CPS version 1.1 22 April 2011

The WISeKey Qualified Services Issuing CA Certification Practice Statement Version 1.0.1 14 April 2009 [PDF] was amended as follows:

The following items were removed from the table in Section 6.2

Individual	CertifyID Qualified Individual (Signing Certificate for Individual)	WISeKey web site, WISeKey appointed Registration Authority	Applicant must present a signed application form, and accompanying identity documentation. Ownership of email address must also be confirmed through an email challenge or other method. Email uniqueness among the group of Individual Qualified user certificate holders will be checked.	Allows certificate owner to digitally sign email messages, documents, and files. Allows relying parties to verify digital signed emails, documents and files, and to send encrypted email to the certificate subscriber. Also allows secure authentication to web sites.
Individual on behalf of-Company	CertifyID Qualified Corporate (Signing Certificate for Corporates)	WISeKey web site, WISeKey appointed Registration Authority	Applicant must present a signed application form, , and accompanying identity documentation. Application must provide documentation indicating their position in the company. The right to use the business name must be proven through documentation or third party databases. Ownership of email address must be confirmed through an email challenge, or other method. In addition, when delivered via an MPKI account, the corporate must prove right to use the domain names that will be restricted to its use. These domain names will be checked to be distinguished within the MPKI account application.	Allows certificate owner to digitally sign email messages, documents, and files proving corporate authorship. Allows relying parties to verify digital signed emails, documents and files, and to send encrypted email to the certificate subscriber. Also allows secure authentication to web sites.

The following sections were deleted:

6.4.1 CertifyID Qualified Individual

Version	*2 (i.e. X.509 version 3)*	
Serial Number	*Unique serial numbers are assigned by the CA*	
Signature Algorithm	Sha1RSA	f
Issuer Distinguished Name		
Common Name (CN)	WISeKey CertifyID Qualified Services CA 1	f

Organisational Unit (OU)	International	f
Organisational Unit (OU)	Copyright (c) 2006 WISeKey SA	
Organisation (O)	WISeKey	f
Country (C)	CH	f
Validity		
Not Before	Time of issue	
Not After	1 – 3 years	f
Subject		
Email (E)	<Subscriber email>	m/e
Common Name (CN)	<Subscriber common name>	m/e
Locality (L)	<Subscriber locality>	o/e
State or Province Name (ST)	<Subscriber state>	o/e
Organisational Unit (OU)	CertifyID Qualified Individual for Aobe	m/f
Organisational Unit (OU)	Copyright (c) 2006 WISeKey SA	o/e
Organisational Unit (OU)	Validated by [Appointed RA] – CertifyID RA Issued via [Client MPKI Subscriber Name]	o/f
Organisational Unit (OU)	<Subscriber organisational unit>	o/e
Country (C)	<Subscriber country code>	m/e
Subject Public Key Info	2048 bit RSA	f

X.509 Extensions

Authority Key Identifier	Extension marked non-critical.
Key Identifier	KeyID=ed 62 b4 e4 fb 29 00 90 55 0f 77 ce 8c e1 24 1b c5 28 87 71
Subject Key Identifier	Extension marked non-critical
Key Identifier	The Subject Key Identifier of the Subject of this certificate.
SMIME Capabilities	[1]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80 [2]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 00 80 [3]SMIME Capability Object ID=1.3.14.3.2.7

	[4]SMIME Capability Object ID=1.2.840.113549.3.7
CRL Distribution Point	Extension marked non-critical.
Fullname	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://public.wisekey.com/crl/wcidqsca1.crl
Authority Information Access	Extension marked non-critical.
	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://public.wisekey.com/crt/wcidqsca1.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.wisekey.com/
Key Usage	Extension marked critical.
	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
Enhanced Key Usage	Document Signing (1.3.6.1.4.1.311.10.3.12) Smart Card Logon (1.3.6.1.4.1.311.20.2.2) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)

6.4.2 CertifyID Qualified Corporate

Version	*2 (i.e. X.509 version 3)*	
Serial Number	*Unique serial numbers are assigned by the CA*	
Signature Algorithm	Sha1RSA	f
Issuer Distinguished Name		
Common Name (CN)	WISeKey CertifyID Qualified Services CA 1	f
Organisational Unit (OU)	International	f
Organisational Unit (OU)	Copyright (c) 2006 WISeKey SA	

Organisation (O)	WISeKey	f
Country (C)	CH	f
Validity		
Not Before	Time of issue	
Not After	1 – 3 years	f
Subject		
Email (E)	<Subscriber email>	o/e
Common Name (CN)	<Subscriber common name>	m/e
Locality (L)	<Subscriber locality>	o/e
State or Province Name (ST)	<Subscriber state>	o/e
Organisational Unit (OU)	Copyright (c) 2006 WISeKey SA	o/e
Organisational Unit (OU)	CertifyID Qualified Corporate	m/f
Organisational Unit (OU)	Validated by [Appointed RA] – CertifyID RA Issued via [Client MPKI subscriber name]	o/f
Organisational Unit (OU)	<Subscriber organisational unit>	
Organisation (O)	<Subscriber organisation name - reserved>	m/e
Country (C)	<Subscriber country code>	m/e
Subject Public Key Info	2048 bit RSA	f

X.509 Extensions

Authority Key Identifier	Extension marked non-critical.
Key Identifier	KeyID=ed 62 b4 e4 fb 29 00 90 55 0f 77 ce 8c e1 24 1b c5 28 87 71
Subject Key Identifier	Extension marked non-critical
Key Identifier	The Subject Key Identifier of the Subject of this certificate.
SMIME Capabilities	[1]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80 [2]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 00 80 [3]SMIME Capability Object ID=1.3.14.3.2.7 [4]SMIME Capability

	Object ID=1.2.840.113549.3.7
CRL Distribution Point	Extension marked non-critical.
Fullname	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://public.wisekey.com/crl/wcidqsca1.crl
Authority Information Access	Extension marked non-critical.
	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://public.wisekey.com/crt/wcidqsca1.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.wisekey.com/
Key Usage	Extension marked critical.
	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
Allowed Enhanced Key Usages	Document Signing (1.3.6.1.4.1.311.10.3.12) Smart Card Logon (1.3.6.1.4.1.311.20.2.2) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)

The following text was changed:

ORIGINAL TEXT	**NEW TEXT IN CPS 1.1**
6.4.3 CertifyID Qualified Individual for Adobe	**6.4.1 CertifyID Qualified Individual for Adobe**
Not After 1 – 3 years m/e	Not After 1 – 3 years m/e
Organisational Unit (OU) Copyright (c) 2006 WISeKey SA o/e Organisational Unit (OU) Validated by [Appointed RA] – CertifyID RA Issued via [Client MPKI Subscriber Name] o/f	Organisational Unit (OU) Copyright (c) 2011 WISeKey SA o/e Organisational Unit (OU) Validated by [Appointed RA] – CertifyID RA Issued via [Client MPKI Subscriber Name] o/e
Certificate Policy [1]Certificate Policy:	REMOVED

Policy Identifier=2.16.756.5.14.4.4.2.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id= CertifyID Qualified Individual for Adobe Qualifier: http://www.wisekey.com/repository [2]Certificate Policy: Policy Identifier=All Issuance Policies (2.16.756.5.14.4.3)	

6.4.4 CertifyID Qualified Corporate for Adobe	**6.4.2 CertifyID Qualified Corporate for Adobe**
Not After 1 – 3 years f	Not After 1 – 3 years o/e
Organisational Unit (OU) CertifyID Qualified Corporate for Adobe m/f Organisational Unit (OU) Validated by [Appointed RA] – CertifyID RA Issued via [Client MPKI subscriber name] o/f	Organisational Unit (OU) CertifyID Qualified Corporate for Adobe m/f Organisational Unit (OU) Validated by [Appointed RA] – CertifyID RA Issued via [Client MPKI subscriber name] o/e
Certificate Policy [1]Certificate Policy: Policy Identifier=2.16.756.5.14.4.4.2.1.4 [1,1]Policy Qualifier Info: Policy Qualifier Id= CertifyID Qualified Corporate for Adobe Qualifier: http://www.wisekey.com/repository [2]Certificate Policy: Policy Identifier=All Issuance Policies (2.16.756.5.14.4.3)	REMOVED

In Section 7.1

The WISeKey Root CPS shall be published at the WISeKey Web site at http://www.wisekey.com/repository/.	The WISeKey Root CPS shall be published via the WISeKey Web site at http://www.wisekey.com/repository/.
The Issuing CA CPS shall be disseminated to WISeKey web site http://www.wisekey.com/repository/.	The Issuing CA CPS shall be disseminated via the WISeKey web site http://www.wisekey.com/repository/.