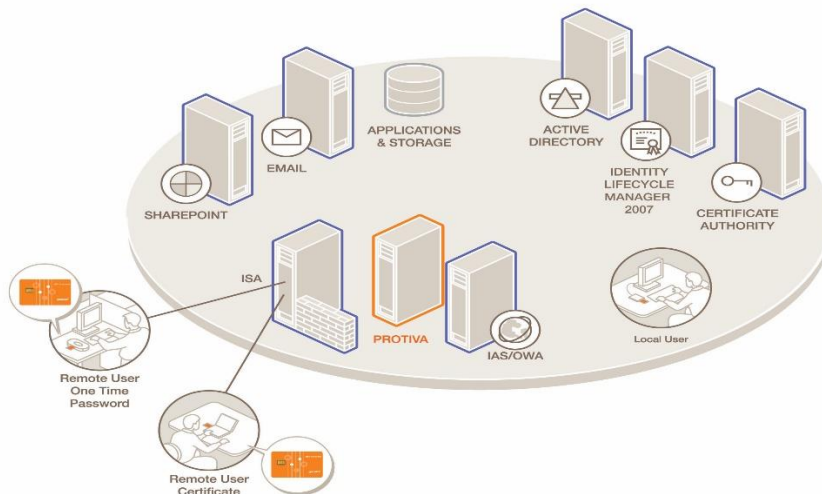


## Gemalto IDPrime .NET V3 Smart Card Technical Specifications



Gemalto .NET puts state of the art technology to the service of organizations committed to take their IT Security and Identity & Access infrastructure to the next level. Two-factor authentication (2FA) solutions help secure your company's digital assets from end to end. Gemalto .NET comes equipped with support for **2 different 2FA technologies: One Time Passwords (OTP) and Digital Certificates (PKI)**. Choose the one that suits you best, or combine both at once for different uses.

With Gemalto .NET you will benefit from **unparalleled level of integration with Microsoft's platforms and solutions**: Support for the Gemalto .NET Smart Cards and Tokens is **built into Windows Vista, 7, 8, 10 and Windows Server 2008, 2012** and available as a Windows Update for Windows XP and Server 2003. Gemalto .NET is also fully compatible with Forefront Edge, Microsoft's **Identity Lifecycle Manager**, Active Directory Domain Services and Certificate Services. With Gemalto .NET implementation of Two Factor Authentication, Encryption and Digital Signature services becomes easier than ever.



### TECHNICAL SPECIFICATIONS

<b>Smart card chip</b>	Chip manufacturer	Infineon
	Chip reference	SLE 88CFX4000P
	ROM memory	80 KB
	EEPROM memory	400 KB

	RAM memory	16 KB
	CPU	RISC 32 bit
	Internal clock	66 MHz
	External clock	up to 10 MHz
	Voltage range	1.62 V - 5.5 V
	Temperature range	-25 C to +85 C
	Technology	CMOS 0.13 microns
	Memory rewrite	> 500 K r/w cycles
	Data retention	>10 years
	Crypto processor	Yes (1408 bit)
	Onboard key generation	Yes
	True Random Number Generator	Yes
Smart card OS	OS type	.NET
	Free EEPROM (approx)	54 KB
	Max # of 1024 certificates	15
	Max # of 2048 certificates	15
	Max I/O speed	223 Kbps, negotiable PPS
Communication protocols	ISO 7816 protocol	T=0
	RMI / Remoting	.NET Remoting
	SConnect	Yes
Cryptographic algorithms	RSA	Yes (up to 2048 bit)
	Elliptic Curves	No
	DES / TDES	Yes
	AES	Yes (256)
	Hash SHA1 / SHA256	Yes
	Hash HMAC / MD5	Yes
Security certifications	Common Criteria	<u>EAL5+ (chip)</u>
	FIPS 140-2	Level 3
Standards	ISO 7816	1, 2,3
	Javacard	No
	Others	ECMA 335
		ISO/IEC 23271
Supported crypto. architectures	Microsoft CAPI	Base CSP v5 to v7
	PKCS#11 for Windows	Yes
	PKCS#11 for Linux	Yes

	PKCS#11 for MacOS	Yes
<b>Microsoft Minidriver</b>	Windows 7,8,10 Server 2008 R2,2013	Microsoft Update (automatic)
	Vista, Server 2008	v5 In the Box & Update
	XP up to SP3, Server 2003	v5 Base CSP & Update
<b>Performance of crypto. operations</b>	Key Gen (CSP)	3.4 s
	Key Gen (P11)	6.9 s
	Import P12 (CSP)	9.1 s
	Import P12 (P11)	7.4 s
	Cached WinLogon (CSP)	1.5 s
	Crypto (CSP)	2.3 s
	Crypto (P11)	4.5 s
	Enumeration (CSP)	4.7 s
	Enumeration (P11)	4.2 s
<b>Supported certificate / data formats</b>	X509 v3	Yes
	PKCS12 / PFX	Yes
	PKCS#15	No
<b>Form factors</b>	Smart Card	Standard (ID1) & SIM (ID000) format
	Hybrid Card (contact + contactless)	Yes
	USB Token	Yes
	USB Token with OTP display	Yes
	USB Token with secure mass storage	Yes
<b>Contactless technologies</b>	MIFARE 1K, 4K, DESFire, Plus	Yes
	HID IClass and/or Prox	Yes
	Legic	Yes
<b>Tools</b>	SDK	Yes
	DAS, vSEC:CMS	Change & unblock PIN, Admin Key & certif. Mgmt