جمهوری اسلامی ایران
مرکز دولتی صدور گواهی الکترونیکی ریشه

معرفی استانداردهای زیرساخت کلید عمومی کشور

طبقه‌بندی: عادی

شماره بازنگری :۱/۰

فهرست مطالب

۱ مقدمه ۴

۲ قلمرو ۴

۳ هدف ۵

۴ معرفی استانداردها ۷

۵ پروفایل‌ها ۱۶

۵-۱ ملزومات پروفایل گواهی‌های الکترونیکی ۱۶

۵-۲ ملزومات پروفایل لیست گواهی‌های باطل شده و نام‌های متمایز کننده ۱۷

۶ الگوریتم‌ها و مکانیزم‌های رمزنگاری ۱۷

۶-۱ ملزومات الگوریتم‌های رمزنگاری ۱۷

۶-۲ دستورالعمل طراحی و ارزیابی الگوریتم‌های رمزنگاری بومی ۱۸

۶-۳ ملزومات احراز هویت دوعامله در زیرساخت کلید عمومی کشور ۱۹

۷ پروتکل‌های مدیریتی ۲۰

۷-۱ پروتکل مدیریت گواهی‌های الکترونیکی ۲۰

۷-۲ پروتکل درخواست گواهی الکترونیکی ۲۰

۸ پروتکل‌های عملیاتی ۲۱

۸-۱ پروتکل‌های OCSP/LDAP/TSP ۲۱

۹ پروتکل تشکیل و اعتبارسنجی زنجیره گواهی ۲۳

۹-۱ پروتکل تشکیل و اعتبارسنجی زنجیره گواهی در زیرساخت کلید عمومی کشور ۲۳

۱۰ ماژول‌های سخت‌افزاری رمزنگاری ۲۵

۱۰-۱ ملزومات امنیتی توکن‌های سخت‌افزاری ۲۵

۱۰-۲ دستورالعمل ارزیابی توکن‌های امنیتی جهت استفاده در زیرساخت کلید عمومی کشور ۲۵

۱۰-۳ ملزومات واسط‌های نرم‌افزاری جهت مدیریت ماژول‌های سخت‌افزاری رمزنگاری ۲۵

۱۱ تجهیز برنامه‌های کاربردی به زیرساخت کلید عمومی ۲۷

۱۱-۱ ملزومات برنامه‌های کاربردی مجهز به زیرساخت کلید عمومی ۲۷

۱۱-۲ دستورالعمل ارزیابی برنامه‌های کاربردی مجهز به زیرساخت کلید عمومی ۲۸

۱۲ موارد دیگر ۲۸

۱۲-۱ ملزومات تدوین سیاست‌ها و دستورالعمل‌های اجرایی مراکز صدور گواهی ۲۸

۱۲-۲ ملزومات رمزنگاری مبتنی بر کلمه عبور ۲۸

۱۲-۳ ملزومات ساختار پیام‌های رمزنگاری (CMS) ۲۹

۱۲-۴ ملزومات ساختار اطلاعات مربوط به کلید خصوصی ۲۹

۱۲-۵ ملزومات ساختار تبادل اطلاعات شخصی ۲۹

۱ مقدمه

زیرساخت کلید عمومی در کشور ایران دارای یک مدل سلسله مراتبی می‌باشد. در چنین مدلی شورای سیاست-گذاری گواهی الکترونیکی کشور موظف به تعیین کلیه سیاست‌ها، استانداردها و دستورالعمل‌ها جهت هماهنگ-سازی، ایجاد یکپارچگی و اعمال نظارت بر کلیه اجزای زیرساخت کلید عمومی کشور شامل کلیه مراکز صدور گواهی ریشه و میانی، دفاتر ثبت نام و تمامی نرم‌افزارها و محصولاتی که مجهز به این زیرساخت شده‌اند، می‌باشد.

در حال حاضر در ایران هیچ نوع استاندارد ملی برای زیرساخت کلید عمومی وجود ندارد، که این به معنی امکان استفاده از تمامی استانداردهای شناخته شده جهانی می‌باشد. بکاربردن استانداردهای زیرساخت کلید عمومی بدون تعیین قلمرو و قالب مشخص و متناسب با نیازمندی‌های زیرساخت کلید عمومی هر کشور و سیاست‌های مرکز ریشه صدور گواهی، مانعی برای اعمال نظارت و ایجاد یکپارچگی و تعامل بین بخش‌های مختلف می‌باشد. لذا ضروری است که تعریفی برای این استانداردها جهت استفاده در زیرساخت کلید عمومی هر کشور وجود داشته باشد.

این گزارش به معرفی استانداردها و دستورالعمل‌های مورد نیاز در زیرساخت کلید عمومی کشور در حوزه‌های مختلف و همچنین به تشریح کاربرد این استانداردها و لزوم وجود یک استاندارد ملی در برخی از این حوزه‌ها جهت تدوین "سند جامع استانداردهای زیرساخت کلید عمومی کشور" می‌پردازد.

بر این اساس گزارش پیش‌رو از بخش‌های ذیل تشکیل شده است:

- در بخش دوم قلمروی مباحث مطرح شده در این گزارش آورده شده است.
- در بخش سوم اهداف و ملزومات وجود استانداردهای ملی در زیرساخت کلید عمومی کشور تشریح شده است.
- در بخش چهارم به معرفی اجمالی استانداردهای زیرساخت کلید عمومی در حوزه‌های مختلف پرداخته شده است.
- در بخش‌های پنجم تا سیزدهم، استانداردهای مورد نیاز در زیرساخت کلید عمومی به تفکیک حوزه‌های مختلف تشریح شده‌اند و به بیان کاربرد هر استاندارد و لزوم وجود استاندارد ملی در برخی از حوزه‌ها پرداخته شده است.

۲ قلمرو

در این گزارش به معرفی استانداردهای مورد نیاز جهت استفاده در زیرساخت کلید عمومی کشور در حوزه‌های قید شده در جدول ذیل پرداخته شده است.

جدول۱ قلمروی استانداردها و دستورالعمل‌های معرفی شده در این گزارش

موارد دیگر	PK-Enabling	ماژول‌های رمزنگاری	پروتکل‌ها	الگوریتم‌ها	پروفایل‌ها
Key Encryption (PKCS#5 & PKCS#8)	Requirements	Security Token Requirements	CMP	Acceptable Algorithms	DN Profile
CMS (PKCS#7)	Validation Program	Security Token Validation Program	CSR/CRMF/CMC	Local Algorithms	Certificate Profile
PFX (PKCS#12)		Acceptable Interfaces	LDAP/OCSP/TSP	Two Factor Authentication	CRL Profile
CP/CPS			Certificate Path Validation		

۳ هدف

در جدول ذیل اهداف و ملزومات استفاده از استانداردهای متناسب با زیرساخت کلید عمومی ملی ایران تشریح شده است.

جدول۲ اهداف و ملزومات تدوین استانداردهای ملی

اهداف	ملزومات
محدودسازی قلمروی اجرایی استانداردهای جهانی	-- هماهنگ‌سازی استانداردهای معتبر جهانی با زیرساخت کلید عمومی کشور
اعمال یکپارچگی و تعامل در زیر ساخت کلید عمومی	-- اطمینان از امکان تعامل بین موجودیت‌های

کشور بین مراکز صدور گواهی الکترونیکی معتبر	زیرساخت کلید عمومی در ایران -- ارزیابی صحیح مشخصات تعاملی بین محصولات زیرساخت کلید عمومی کشور
حمایت از شرکت‌های داخلی جهت تولید محصولات مرتبط با PKI و ارتقای زیر ساخت کلید عمومی ملی	استفاده از کلیه توانمندی‌های کشور جهت تولید محصولات قابل اعتماد مرتبط با زیرساخت کلید عمومی منطبق با استانداردها و دستورالعمل‌های ارائه شده در این گزارش
اعمال نظارت کامل بر کلیه اجزای زیرساخت کلید عمومی کشور	-- تدوین و تصویب استانداردها و دستورالعمل‌های ارائه شده در این گزارش -- پیاده سازی و اعمال این استانداردها در زیرساخت کلید عمومی کشور -- راه‌اندازی آزمایشگاه‌های داخلی جهت ارزیابی تمامی محصولات مرتبط با زیرساخت کلید عمومی

۴ معرفی استانداردها

در این بخش استانداردها و دستورالعمل‌های مورد نیاز در زیرساخت کلید عمومی کشور بطور خلاصه معرفی شده‌اند. در جدول ۴ این استانداردها در حوزه‌های مختلف معرفی شده و استانداردها و اسناد شناخته شده جهانی متناظر با هر استاندارد در ستون مراجع قید شده است. همچنین تشریح هر استاندارد بطور خلاصه در ستون توضیحات آورده شده و معانی واژه‌های بکار رفته در ستون **نام استاندارد** ، در جدول ۳ آورده شده است.

جدول۳ معانی واژه‌های بکاررفته در ستون نام استاندارد

واژه	معنی
ملزومات	بیانگر استانداردی می‌باشد که در آن ملزومات لازم برای یک شی (ساختار اطلاعاتی، ماژول سخت‌افزاری، برنامه کاربردی و یا یک فرآیند) تعیین شده است.
دستورالعمل	بیانگر استانداردی است که در آن روش اجرایی انجام یک فرآیند تشریح شده است.
پروتکل	بیانگر استانداردی است که در آن یک پروتکل خاص شامل ملزومات و روش اجرایی انجام یک فرآیند یا تراکنش تشریح شده است.

جدول۴ معرفی استانداردها و دستورالعمل‌های مورد نیاز در زیرساخت کلید عمومی کشور

نوع استاندارد	نام استاندارد	مراجع	توضیحات
پروفایل‌ها	**ملزومات پروفایل گواهی‌های الکترونیکی**	RFC 5280	در حال حاضر ملزومات پروفایل گواهی‌های الکترونیکی، CRL و نام‌های متمایز کننده در قالب سند جامع پروفایل‌های زیرساخت کلید عمومی کشور توسط مرکز دولتی صدور گواهی ریشه تدوین شده است.
	ملزومات پروفایل لیست گواهی‌های باطل شده	RFC 5280	
	ملزومات پروفایل نام‌های متمایز کننده (DN)	RFC 2256	
	ملزومات الگوریتم‌های رمزنگاری	RSA : PKCS#1 FIPS 186-2 FIPS 186-3	معرفی الگوریتم‌های رمزنگاری پذیرفته شده در زیرساخت کلید عمومی کشور شامل: الگوریتم‌های متقارن و نامتقارن، توابع درهم‌ساز، کدهای تشخیص

نوع استاندارد	نام استاندارد	مراجع	توضیحات
الگوریتم‌های رمزنگاری		ECDSA: PKCS#13 FIPS 186-2 FIPS 186-3	اصالت پیام و مولدهای اعداد تصادفی -- در صورت نیاز تعیین پارمترها و طول کلید مناسب برای هر الگوریتم
		AES: ISO/IEC 18033-3 FIPS 197 NIST sp 800-38A NIST sp 800-38C NIST sp 800-38D	
		TDES: ISO/IEC 18033-3 NIST sp 800-67	

نوع استاندارد	نام استاندارد	مراجع	توضیحات
		NIST sp 800-38A : SHA1 & SHA2 NIST sp 180-3	
		:MAC FIPS 113 NIST 800-38B NIST 800-38C	
		: HMAC-SHA FIPS 198-1	

نوع استاندارد	نام استاندارد	مراجع	توضیحات
		: PRNG FIPS 186-2 ANSI X9.31	
	ملزومات مکانیزم‌های احراز هویت دوعامله در زیرساخت کلید عمومی کشور	FIPS 196	معرفی و ارائه یک مکانیزم احراز هویت کلید عمومی مبتنی بر چالش و پاسخ و تعیین ملزومات پیاده‌سازی این مکانیزم بصورت دوعامله جهت استفاده در زیرساخت کلید عمومی کشور و نرم-افزارهای PKE
	دستورالعمل ارزیابی الگوریتم‌های رمزنگاری	Cryptographic Algorithm Validation Program (CAVP)	ارائه یک روش اجرایی جهت ارزیابی الگوریتم‌های رمزنگاری

نوع استاندارد	نام استاندارد	مراجع	توضیحات
پروتکل‌های مدیریتی	پروتکل مدیریت گواهی‌های الکترونیکی (CMP)	RFC 4210	استاندارد پروتکل مدیریت گواهی‌های الکترونیکی جهت تشریح چگونگی تعامل بین اجزای زیرساخت کلید عمومی و ساختار اطلاعات رد و بدل شده بین این اجزا
	پروتکل درخواست گواهی در زیرساخت کلید عمومی کشور (CSR, CRMF, CMC)	PKCS#10 (CSR) RFC 4211 (CRMF) RFC 5272, RFC 5273, RFC 5274 (CMC)	استاندارد پروتکل درخواست گواهی جهت ایجاد یکپارچگی و هماهنگی بین دفاتر ثبت‌نام و مراکز صدور گواهی مختلف و قابلیت اعمال نظارت و کنترل کامل بر دفاتر ثبت‌نام

نوع استاندارد	نام استاندارد	مراجع	توضیحات
پروتکل‌های عملیاتی	**پروتکل‌های** OCSP/LDAP/TSP	RFC 2560 RFC 3161 RFC 3494	استانداردهای پذیرفته شده برای پروتکل‌های عملیاتی OCSP، LDAP و TSP
پروتکل تشکیل و اعتبارسنجی زنجیره گواهی	پروتکل تشکیل و اعتبارسنجی زنجیره گواهی در زیرساخت کلید عمومی کشور	RFC 5280	استاندارد پروتکل تشکیل و اعتبارسنجی زنجیره گواهی جهت استفاده در نرم‌افزارهای PKE
ماژول‌های سخت‌افزاری رمزنگاری	ملزومات امنیتی توکن‌های سخت‌افزاری	FIPS 140-2 C.C Smart card Protection Profile PKCS#11	بیان‌کننده ملزومات امنیتی توکن‌های سخت‌افزاری جهت استفاده در زیرساخت کلید عمومی کشور

نوع استاندارد	نام استاندارد	مراجع	توضیحات
	دستورالعمل ارزیابی توکن‌های سخت‌افزاری	NIST Cryptographic Module Validation Program (CMPV)	دستورالعمل ارزیابی توکن‌های امنیتی بر اساس استاندارد ملی توکن‌های امنیتی جهت استفاده در آزمایشگاه‌های ارزیابی محصولات PKE
	ملزومات واسط‌های نرم‌افزاری جهت مدیریت ماژول‌های سخت‌افزاری رمزنگاری	PKCS#11 Cryptographic Service Provider (CSP) Key Storage Provider (KSP)	معرفی واسط‌های برنامه‌نویسی پذیرفته شده جهت برقراری ارتباط با ماژول-های رمزنگاری و مدیریت آن‌ها در زیرساخت کلید عمومی کشور
تجهیز برنامه‌های کاربردی به زیرساخت کلید عمومی (PK-Enabling)	ملزومات برنامه‌های کاربردی مجهز به زیرساخت کلید عمومی کشور (PKE Applications)	مستندات معتبر در زمینه PK-Enabling از جمله مستندات DOD	بیان‌کننده ملزومات امنیتی مورد نیاز برای نرم‌افزارهای مجهز شده به زیرساخت کلید عمومی کشور (نرم‌افزارهای PKE)
	دستورالعمل ارزیابی برنامه‌های کاربردی مجهز به زیرساخت کلید عمومی کشور	مستندات معتبر در زمینه PK-Enabling از جمله مستندات DOD	دستورالعمل ارزیابی نرم‌افزارهای PKE بر اساس استاندارد ملزومات برنامه‌های کاربردی مجهز شده به زیرساخت کلید عمومی کشور، جهت استفاده در آزمایشگاه‌های ارزیابی محصولات

نوع استاندارد	نام استاندارد	مراجع	توضیحات
			PKE
موارد دیگر	ملزومات ساختار پیام‌های رمزنگاری (CMS)	PKCS#7 RFC 2315	ارائه دهنده ساختار پیام‌های رمزنگاری جهت استفاده در زیرساخت کلید عمومی کشور جهت ایجاد یکپارچگی و تعامل بین نرم‌افزارهای PKE و اعمال نظارت و کنترل کامل بر نرم‌افزارهای PKE
	ملزومات تدوین سیاست‌ها و دستورالعمل-های اجرایی مراکز صدور گواهی	RFC 3647	بیان کننده ساختار و قالب تدوین CP و CPS
	ملزومات رمزنگاری مبتنی بر کلمه عبور	PKCS#5	بیان‌کننده مکانیزم رمزگذاری کلید خصوصی بر اساس یک روش مبتنی بر کلمه عبور
	ملزومات ساختار اطلاعات مربوط به کلید خصوصی	PKCS#8	ارائه دهنده یک ساختار جهت نگهداری کلید خصوصی
	ملزومات ساختار تبادل اطلاعات شخصی		ارائه دهنده یک ساختار جهت نگهداری و انتقال اطلاعات شخصی شامل کلید

نوع استاندارد	نام استاندارد	مراجع	توضیحات
	(شامل کلید خصوصی و گواهی‌های الکترونیکی)	PKCS#12	خصوصی و گواهی‌های الکترونیکی بصورت امن

۵ پروفایل‌ها

۵-۱ ملزومات پروفایل گواهی‌های الکترونیکی

یکی از بزرگترین مشکلات مراکز صدور گواهی الکترونیکی ناهماهنگی استفاده از گواهی‌های صادر شده توسط آنها می‌باشد، بدین منظور که اگر کاربری چندین گواهی با کاربرد یکسان از مراکز صدور گواهی الکترونیکی متفاوت داشته باشد بدلیل ناهماهنگی آنها نمی‌تواند از گواهی‌های خود بطور یکسان استفاده نماید.

با توجه به انواع گواهی الکترونیکی مورد نیاز در زیرساخت کلید عمومی کشور و کاربردهای تعریف شده برای این گواهی‌ها، وجود یک استاندارد یا دستورالعمل جهت تعریف قالب یا پروفایل این گواهی‌های الکترونیکی، کاملاً ضروری می‌باشد. در حال حاضر این استاندارد در قالب سند جامع پروفایل‌های زیرساخت کلید عمومی کشور توسط مرکز دولتی صدور گواهی ریشه تدوین شده است و کلیه مراکز صدور گواهی میانی موجود در ساختار سلسله مراتبی مراکز صدور گواهی کشور، می‌بایست انواع گواهی‌های الکترونیکی را منطبق با این سند اجرایی صادر نمایند.

۵-۲ ملزومات پروفایل لیست گواهی‌های باطل شده و نام‌های متمایز کننده

به منظور یکپارچه‌سازی و هماهنگی بین مراکز صدور گواهی در زیرساخت کلید عمومی کشور جهت اعلام وضعیت گواهی‌های الکترونیکی از طریق لیست گواهی‌های باطل شده یا CRL وهمچنین نحوه نام‌گذاری گواهی‌های الکترونیکی، وجود یک استاندارد جهت تعریف قالب یا پروفایل لیست گواهی‌های باطل شده که در آن چگونگی مقداردهی فیلدهای اصلی و فیلدهای الحاقی CRL و CRL Entry تشریح شده و همچنین نحوه نام‌گذاری گواهی-های الکترونیکی (مقداردهی فیلدهای SubjectName و IssuerName) تعریف شده باشد، کاملاً ضروری به نظر می‌رسد. در حال حاضر این استاندارد در قالب سند جامع پروفایل‌های زیرساخت کلید عمومی کشور، توسط مرکز دولتی صدور گواهی ریشه تدوین شده است و کلیه مراکز صدور گواهی میانی موجود در ساختار سلسله مراتبی مراکز صدور گواهی کشور، می‌بایست لیست گواهی‌های باطل شده را منطبق با این سند تولید و منتشر نمایند و نام‌گذاری گواهی‌های الکترونیکی صادر شده را منطبق با این سند انجام دهند.

۶ الگوریتم‌ها و مکانیزم‌های رمزنگاری

۶-۱ ملزومات الگوریتم‌های رمزنگاری

بطور کلی انواع الگوریتم‌های رمزنگاری مورد استفاده در یک زیرساخت کلید عمومی عبارتند از:

۱. **الگوریتم‌های رمزنگاری نامتقارن یا کلید عمومی:** این الگوریتم بعنوان الگوریتم‌های اصلی در زیرساخت کلید عمومی مورد استفاده قرار می‌گیرند و بطور معمول جهت امضای دیجیتال و تبادل و توافق کلیدهای متقارن بکار می‌روند. به عبارت دیگر از این الگوریتم‌ها جهت اعمال سرویس‌های امنیتی احراز هویت[1]، تمامیت[2]، انکارناپذیری[3] و محرمانگی[4] استفاده می‌شود.

۲. **الگوریتم‌های رمزنگاری متقارن:** این الگوریتم‌ها برخلاف الگوریتم‌های کلید عمومی از یک کلید مشترک و متقارن جهت انجام عملیات رمزنگاری استفاده می‌نمایند و در یک زیرساخت کلید عمومی جهت رمزگذاری کلید خصوصی و حجم اطلاعات بزرگ مورد استفاده قرار می‌گیرند. بنابراین الگوریتم‌های

[1] Authentication
[2] Integrity
[3] Non Repudiation
[4] Privacy

رمزنگاری متقارن در یک زیرساخت کلید عمومی جهت اعمال سرویس امنیتی محرمانگی مورد استفاده قرار می‌گیرند.

۳. **توابع درهم‌ساز:** از توابع‌درهم‌ساز در یک زیرساخت کلید عمومی جهت انجام عملیات امضای دیجیتال و اعمال سرویس امنیتی تمامیت استفاده می‌شود.

۴. **مولدهای اعداد تصادفی:** مولدهای اعداد تصادفی بطور معمول جهت انجام عملیات تولید کلیدهای متقارن و نامتقارن مورد استفاده قرار می‌گیرند و همچنین تولید کننده عامل تصادفی در الگوریتم‌های رمزنگاری تصادفی و غیر قطعی می‌باشند.

با توجه به وجود انواع حملات رمزشکنی و تحلیل رمز روی الگوریتم‌های رمزنگاری مختلف و لزوم استفاده از پارامترها و طول کلید مناسب برای این الگوریتم‌ها، وجود یک استاندارد ملی در زیرساخت کلید عمومی کشور جهت تعیین الگوریتم‌های رمزنگاری پذیرفته شده که امنیت مورد انتظار را برآورده سازند و تعریف پارامترها و طول کلید مناسب برای این الگوریتم‌ها جهت استفاده در مراکز صدور گواهی، دفاتر ثبت‌نام و نرم‌افزارهای مجهز به زیرساخت کلید عمومی، کاملاً ضروری بنظر می‌رسد.

۶-۲ دستورالعمل طراحی و ارزیابی الگوریتم‌های رمزنگاری بومی

اصل کرکهف[1]، یک اصل و قانون بسیار مهم در سیستم‌های رمزنگاری می‌باشد که بیان می‌دارد : "جزئیات الگوریتم-های رمزنگاری می‌بایست آشکار باشند و فقط کلیدهای رمز، سری و محرمانه هستند."

استدلال زیر عقلانیت نهفته در اصل کرکهف را روشن‌تر می‌کند:

الف) هرگاه کلید رمز در اثر خیانت یا سهل‌انگاری یا هر عامل دیگر افشا شود، با تغییر کلید رمز جلوی ضرر گرفته می‌شود ولی وجود روزنه و نفوذ در یک سیستم رمزنگاری امنیت کل سامانه را از بین می‌برد و تنها راه، تغییر سریع سیستم رمزنگاری است که این تغییر هرگز به راحتی و در زمان کوتاه میسر نخواهد بود.

ب) هرگاه روشی برای سال‌ها در معرض افکار پژوهشگران و متخصصان این فن باشد و به طرق علمی و عملی به چالش کشیده شود و هیچ تلاشی در شکستن آن به ثمر نرسد، می‌توان احتمال داد که سیستم مورد نظر بقدر کافی امن بوده است.

در حال حاضر مشاهده می‌شود که در برخی از سازمان‌ها و ارگان‌ها در سطح کشور از الگوریتم‌های رمزنگاری بومی بدون وجود ساز وکار مشخص برای طراحی و ارزیابی این الگوریتم‌ها، استفاده می‌شود و این تمایل و گرایش جهت استفاده از الگوریتم‌های بومی جهت بالا بردن سطح امنیت و اطمینان در بسترهای اطلاعاتی، در بخش‌های مختلف

[1] Kerchoff

دیده می‌شود. استفاده از الگوریتم‌های رمزنگاری بومی بدون رعایت اصل کرکهف، آسیب‌پذیری امنیتی بسیار بالایی بوجود می‌آورد و وجود یک استاندارد یا دستورالعمل جهت ترسیم ساز وکار طراحی و ارزیابی الگوریتم‌های رمزنگاری بومی در صورت نیاز به استفاده از این الگوریتم‌ها در زیرساخت کلید عمومی کشور ضروری بنظر می‌رسد.

۶-۳ ملزومات احراز هویت دوعامله در زیرساخت کلید عمومی کشور

"احراز هویت" روش یا مکانیزمی است که بر اساس آن هر موجودیت (مثل یک پروسه یا شخص) بررسی می‌کند که موجودیت طرف مقابل همانی است که ادعا می‌کند یا یک اخلال‌گر ثالث است که خود را به جای طرف واقعی جا زده است. کاربرد واژگان "احراز هویت" در مورد اشیایی مثل فایل‌ها، برنامه‌های اجرایی و اسناد و مدارک، اشاره به روشی است که بر اساس آن اصالت و درستی آن شیء اثبات می‌شود. احراز هویت در مورد افراد، روشی برای تشخیص هویت واقعی آنان و اثبات درستی یا نادرستی ادعای آن‌ها در خصوص معرفی خودشان است.

در دنیای امنیت داده‌ها واژه مخففی به نام AAA یا A3 وجود دارد که معنای این کوته‌واژه پرکاربرد عبارت است از:

- **اولین A : Authentication** مکانیزمی که بر اساس آن پروسه‌ها هویت حقیقی یا حقوقی کاربران خود را اثبات می‌کنند.
- **دومین A: Authorization** مکانیزمی که بر اساس آن مشخص می‌شود کاربری که هویت او احراز شده، مجوز انجام چه کارها و عملیاتی را دارد.
- **سومین A: Accounting** مکانیزمی که بر اساس آن مشخص می‌شود پروسه یا کاربر چه سهمی از منابع سیستمی و خدمات را می‌برد و آیا در ازای دریافت سهم خدمات، حق و حساب آن را پرداخت کرده است یا خیر.

مهمترین و اولین بخش از عملیات A3 همان عملیات احراز هویت می‌باشد که کابرد ویژه‌ای در زیرساخت کلید عمومی و نرم‌افزارهایی که به این زیرساخت مجهز شده‌اند (نرم‌افزارهای PKE) دارد. عملیات احراز هویت در زیرساخت کلید عمومی و نرم‌افزارهای PKE بدلیل حساسیت امنیتی بالای این نرم‌افزارها می‌بایست بصورت دو عامله صورت گیرد. احراز هویت دوعامله به معنی احراز هویت یک فرد بواسطه "آن چیزی که دارد" و " آن چیزی که می‌داند" می‌باشد. در واقع احراز هویت دوعامله از طریق یک ماژول سخت‌افزاری رمزنگاری مانند توکن امنیتی و با وارد کرد کلمه عبور این ماژول و با استفاده مکانیزم احراز هویت تعریف شده برای این ماژول صورت می‌گیرد.

بنابراین وجود یک استاندارد امنیتی برای احراز هویت دوعامله که تعیین کننده یک مکانیزم احراز هویت امن کلید عمومی که مبتنی بر یک روش چالش و پاسخ باشد و در آن ملزومات پیاده‌سازی این مکانیزم بصورت دوعامله قید شده باشد، لازم و ضروری است.

۷ پروتکل‌های مدیریتی

۷-۱ پروتکل مدیریت گواهی‌های الکترونیکی

در پروتکل CMP[1] چگونگی ارتباط و تعامل بین موجودیت‌های مختلف یک زیرساخت کلید عمومی، مدیریت گواهی‌های الکترونیکی و همچنین ساختار اطلاعات رد و بدل شده بین این موجودیت‌ها تعیین می‌گردد. بعنوان مثال در این پروتکل نحوه تعامل بین موجودیت‌های نهایی و یا دفاتر ثبت‌نام با مراکز صدور گواهی و ساختار اطلاعات رد و بدل شده بین آن‌ها شامل درخواست صدور و ابطال گواهی و تجدید و بازیابی کلید تشریح شده است. البته ساختار کامل اطلاعات درخواست صدور گواهی در RFC 4211 و در قالب استاندارد CRMF قید شده است.

به منظور اعمال یکپارچگی و تعامل بین موجودیت‌های مختلف زیرساخت کلید عمومی ملی و هماهنگ‌سازی دفاتر ثبت‌نام در ارگان‌های مختلف با مراکز صدور گواهی مختلف، وجود یک استاندارد ملی برای پروتکل مدیریت گواهی-های الکترونیکی منطبق با سند RFC 4210 مورد نیاز می‌باشد. در صورت وجود یک استاندارد ملی تعریف شده برای تعامل بین اجزای زیرساخت کلید عمومی کشور و ساختار اطلاعات رد و بدل شده بین آن‌ها، اعمال نظارت و کنترل بر فعالیت دفاتر ثبت‌نام و مراکز صدور گواهی تسهیل شده و قابلیت اعمال یکپارچگی و هماهنگی بین این ارگان‌ها امکان‌پذیر می‌گردد.

۷-۲ پروتکل درخواست گواهی الکترونیکی

در پروتکل درخواست گواهی، ساختار اطلاعات یک درخواست صدور گواهی و نحوه ارائه آن به مرکز صدور گواهی به همراه ملزومات امنیتی لازم برای ارائه این درخواست تشریح می‌گردد. در حالت کلی ارائه یک درخواست گواهی به دوشکل ذیل امکان‌پذیر است:

۱. درخواست ساده PKI منطبق با استاندارد PKCS#10 که به آن CSR گفته می‌شود و شامل کلید عمومی و مشخصات مالک گواهی (SubjectName) است.
۲. درخواست کامل PKI که ممکن است شامل یک یا چند CSR، CRMF[2] یا دیگر ساختارهای درخواست گواهی در قالب استاندارد CMS[3] باشد (استاندارد CMS در بخش ۱۳-۳ شرح داده شده است). به این نوع درخواست CMC[4] گفته می‌شود.

یک درخواست ساده PKI یا CSR بطور معمول جهت اثبات مالکیت کلید خصوصی (POP)[5] مورد استفاده قرار می-گیرد و معمولاً توسط موجودیت نهایی یا مالک گواهی تولید می‌گردد؛ بدین ترتیب که پس از انجام عملیات تولید زوج کلید، کلید عمومی به همراه مشخصات مالک گواهی می‌بایست در قالب استاندارد PKCS#10 با استفاده از کلید

[1] Certificate Management Protocol
[2] Certificate Request Message Format
[3] Cryptographic Message Syntax
[4] Certificate Management over CMS
[5] Proof of Possession

خصوصی، امضا شده و نتیجه در قالب فایل CSR در اختیار RA یا CA قرار گیرد و برای RA یا CA با انجام عملیات تصدیق امضای CSR با استفاده از کلید عمومی موجود در آن، مالکیت کلید خصوصی درخواست کننده گواهی احراز می‌گردد.

یک درخواست کامل PKI معمولاً جهت تنظیم یک درخواست کامل صدور گواهی توسط دفاتر ثبت‌نام (RA) مورد استفاده قرار می‌گیرد. در این درخواست می‌بایست اطلاعات موجود در CSR به همراه اطلاعات تکمیلی دیگر در قالب استاندارد CRMF و منطبق با RFC 4211 شکل گرفته و با امضای این اطلاعات توسط RA ، یک درخواست کامل صدور گواهی جهت ارائه به CA تولید گردد.

به طو کلی ایجاد یک درخواست کامل صدور گواهی شامل مراحل ذیل می‌باشد:

۱. کلید عمومی درخواست کننده گواهی به همراه تمام یا بخشی از مشخصات مالک گواهی (SubjectName) و دیگر فیلدهای درخواست شده گواهی و اطلاعات تکمیلی دیگر منطبق با استاندارد پروتکل درخواست گواهی توسط RA تنظیم و ثبت می‌گردد.
۲. عملیات اثبات مالکیت کلید خصوصی متناظر با کلید عمومی موجود در درخواست (POP) صورت می‌گیرد.
۳. اطلاعات تکمیلی دیگر به همراه نتیجه عملیات POP و ساختار درخواست گواهی توسط RA ترکیب می‌گردند.
۴. درخواست تنظیم شده می‌بایست بصورت امن برای CA ارسال گردد. چگونگی ارسال امن این درخواست می‌بایست در استاندارد پروتکل درخواست گواهی مشخص گردد.

در زیرساخت کلید عمومی کشور جهت ایجاد هماهنگی و یکپارچگی بین دفاتر ثبت‌نام و مراکز صدور گواهی مختلف و همچنین امکان اعمال نظارت و کنترل کامل بر فعالیت‌های دفاتر ثبت‌نام، وجود یک استاندارد ملی برای پروتکل درخواست گواهی که در آن ساختار یک درخواست کامل صدور گواهی و ملزومات امنیتی چگونگی ارائه این درخواست به مراکز صدور گواهی قید شده باشد، ضروری بنظر می‌رسد.

۸ پروتکل‌های عملیاتی

۸-۱ پروتکل‌های OCSP/LDAP/TSP

۸-۱-۱ پروتکل OCSP

پروتکل OCSP[1] یک پروتکل کارا جهت پی بردن به وضعیت جاری گواهی کاربر (ابطال یا عدم ابطال گواهی) بدون نیاز به دریافت و بررسی CRL می‌باشد. پروتکل OCSP اطلاعاتی که لازم است بین نرم‌افزار کاربر (سرویس گیرنده OCSP[2]) و سروری که وضعیت گواهی را گزارش می‌دهد (پاسخگوی OCSP[3])، رد بدل شود را فراهم می‌کند. در واقع پروتکل OCSP به نرم‌افزارهایی که با گواهی سر و کار دارند (کاربران گواهی) این امکان را می‌دهد که وضعیت ابطال و یا عدم ابطال این گواهی را بررسی کنند. سرویس‌گیرنده OCSP جهت پی‌بردن به وضعیت گواهی، یک درخواست وضعیت[4] تنظیم کرده وآنرا برای پاسخ دهنده OCSP ارسال می‌کند. پاسخ‌گوی OCSP با دریافت درخواست و انجام پردازش روی آن، در صورت امکان وضعیت جاری گواهی را بعنوان پاسخ به درخواست سرویس-گیرنده OCSP ، تنظیم و برای او ارسال می‌نماید.

در صورت استفاده از پروتکل OCSP در زیرساخت کلید عمومی کشور، پیاده‌سازی این پروتکل در سمت مراکز صدور گواهی (سرور پاسخگوی OCSP) و در سمت نرم‌افزارهای مجهز شده به زیرساخت کلید عمومی یا نرم‌افزارهای PKE (سرویس‌گیرنده OCSP) می‌بایست منطبق با RFC 2560 صورت گیرد.

۸-۱-۲ پروتکل LDAP

یکی از اجزای زیرساخت کلید عمومی، مخزن[5] گواهی می‌باشد. گواهی‌های صادر شده و آخرین نسخه لیست گواهی باطل شده (CRL) توسط CA در این مخزن گواهی ذخیره می‌گردد. در حقیقت مخزن گواهی سیستمی می‌باشد که برای دسترسی سریع کاربران به گواهی‌ها و CRL در نظر گرفته شده است. اطلاعات منتشر شده در بخش مخزن می‌بایست برای عموم قابل دسترسی باشد و این دسترسی بصورت فقط خواندنی[6] است.

بطور معمول جهت پیاده‌سازی مخزن از پروتکل LDAP [7] استفاده می‌شود. پیاده‌سازی پروتکل LDAP در زیرساخت کلید عمومی کشور می‌بایست منطبق با RFC 3494 صورت پذیرد.

۸-۱-۳ پروتکل TSP

پروتکل TSP [8] یک پروتکل رمزنگاری جهت اعتبارسنجی مهر زمانی با استفاده از گواهی‌های X509 در یک زیرساخت کلید عمومی می‌باشد. با استفاده از یک مهر زمانی از طریق امضای دیجیتال می‌توان اثبات نمود یک بخش از اطلاعات الکترونیکی در یک زمان خاص و یا قبل از یک زمان خاص موجود بوده و یا ثبت شده است.

---

[1] Online Certificate Status Protocol
[2] OCSP Client
[3] OCSP Responder
[4] Status Request
[5] Repository
[6] Read Only
[7] Lightweight Directory Access Protocol
[8] Time Stamp Protocol

در صورت استفاده از پروتکل TSP در زیرساخت کلید عمومی کشور، پیاده‌سازی این پروتکل می‌بایست منطبق با RFC 3161 صورت گیرد.

۹ پروتکل تشکیل و اعتبارسنجی زنجیره گواهی

۹-۱ پروتکل تشکیل و اعتبارسنجی زنجیره گواهی در زیرساخت کلید عمومی کشور

در یک زیرساخت کلید عمومی از طریق گواهی‌های X509 ، مشخصات یک موجودیت به کلید عمومی رمزنگاری این موجودیت پیوند داده می‌شود. یکی از مهمترین قابلیت‌هایی که یک نرم‌افزار مجهز به زیرساخت کلید عمومی (PKE[1]) می‌بایست پشتیبانی نماید، فرآیند تشکیل و اعتبارسنجی زنجیره گواهی می‌باشد. از طریق این فرآیند می‌توان دریافت که به یک گواهی الکترونیکی جهت استفاده در یک نرم‌افزار خاص می‌توان اعتماد نمود یا خیر. به عبارت دیگر در این فرآیند درستی پیوند بین مشخصات مالک گواهی و کلید عمومی او بررسی می‌گردد.

جهت اعتبارسنجی یک گواهی الکترونیکی، می‌بایست قابلیت تشکیل زنجیره گواهی بصورت خودکار توسط نرم‌افزار PKE پشتیبانی شود. در یک زنجیره گواهی، هر گواهی توسط صادر کننده این گواهی امضا شده است و این زنجیره، از گواهی کاربر یا موجودیت نهایی تا گواهی متعلق به مرکز ریشه صدور گواهی امتداد دارد. بعنوان مثال یک زنجیره گواهی ممکن است شامل گواهی کاربر (User) که توسط صادر کننده این گواهی (CA) امضا شده، گواهی CA که توسط صادر کننده این گواهی (Root CA) امضا شده و گواهی متعلق به مرکز ریشه صدور گواهی (Root CA) که توسط خودش امضا شده است (Self_Signed)، باشد.

Root CA $\rightarrow$ CA $\rightarrow$ User

در یک زنجیره گواهی جهت بررسی اعتبار هر گواهی **حداقل** می‌بایست پردازش‌های ذیل صورت پذیرد:

۱. بررسی وجود یا عدم وجود صادر کننده گواهی مورد نظر (Name chaining)
۲. بررسی اعتبار امضای گواهی مورد نظر توسط کلید عمومی گواهی صادر کننده (Signature chaining)
۳. بررسی تاریخ شروع و پایان اعتبار گواهی (Certificate Validity)
۴. بررسی وجود و اعتبار CRL های موجود در زنجیره گواهی (Full CRL)
۵. بررسی اینکه گواهی مورد نظر باطل شده است یا خیر (Check Status)

این بررسی اعتبار، از گواهی موجودیت نهایی شروع شده و با بررسی اعتبار گواهی و CRL متعلق به صادر کننده گواهی کاربر و سطوح بالاتر زنجیره گواهی ادامه پیدا می‌کند و با بررسی اعتبار گواهی مرکز ریشه (این گواهی خود

[1] PK-Enabled

امضا[1] است)، پایان می‌یابد.

در فرآیند اعتبارسنجی زنجیره گواهی در زیرساخت کلید عمومی کشور، علاوه بر موارد فوق می‌بایست پردازش‌های دیگری نیز با توجه به سیاست‌های مرکز دولتی صدور گواهی ریشه صورت پذیرد. بعنوان مثال پردازش الحاقیه‌های[2] Basic Constraints ، Key Usage و دیگر الحاقیه‌های گواهی می‌بایست منطبق با سیاست‌های مرکز ریشه صورت پذیرد. بنابراین وجود یک استاندارد بومی در کشور جهت تعیین ملزومات الگوریتم تشکیل و اعتبارسنجی زنجیره گواهی ضروری بنظر می‌رسد. در سند RFC 5280 یک مکانیزم جامع جهت اعتبارسنجی زنجیره گواهی ارائه شده است که این مکانیزم می‌بایست متناسب با زیرساخت کلید عمومی کشور طراحی گردد.

[1] Self Signed
[2] Extension

۱۰ ماژول‌های سخت‌افزاری رمزنگاری

۱۰-۱ ملزومات امنیتی توکن‌های سخت‌افزاری

توکن‌های امنیتی نوع خاصی از ماژول‌های رمزنگاری می‌باشند که نقش مهمی در امنیت بسترهای اطلاعاتی ایفا می‌کنند. انجام مکانیزم‌های مختلف رمزنگاری توسط توکن‌های امنیتی امکان‌پذیر می‌باشد و در این ماژول‌ها اطلاعات محرمانه کاربران از جمله کلیدهای رمزنگاری و کلمات عبور ذخیره می‌گردد، بنابراین می‌بایست در آن‌ها تمهیدات امنیتی لازم جهت مقابله با دسترسی‌های غیر مجاز، شنود، حملات رمزشکنی و حملات فیزیکی مختلف اندیشیده شده باشد. در استانداردهای امنیتی مختلف از جمله FIPS 140-2 ملزومات امنیتی مورد نیاز برای ماژول‌های سخت‌افزاری رمزنگاری تشریح شده است و آزمایشگاه‌های ارزیابی ماژول‌های رمزنگاری بر اساس این استانداردها برنامه ارزیابی خود را طراحی نموده و ماژول مورد نظر را مورد ارزیابی قرار می‌دهند.

با توجه به اهمیت و لزوم استفاده از توکن‌های امنیتی مورد اعتماد در زیرساخت کلید عمومی کشور و در نرم‌افزارهای مجهز شده به زیرساخت کلید عمومی و راه‌اندازی آزمایشگاه‌های داخلی جهت ارزیابی توکن‌های امنیتی، وجود یک استاندارد ملی برای توکن‌های امنیتی کاملاً ضروری به نظر می‌رسد. برای این استاندارد می‌بایست سطوح امنیتی مختلف تعریف شده و به تناسب این سطوح امنیتی، ملزومات مورد نیاز جهت اعمال در توکن‌های امنیتی در حوزه‌های مختلفی از جمله نقش‌ها و احراز هویت، مدل‌های حالت، امنیت فیزیکی، محیط عملیاتی، مدیریت کلیدهای رمزنگاری، کنترل کیفیت و آزمون خودکار، ضمانت طراحی و اقدامات متقابل در برابر حملات کانال جانبی، تشریح شده باشد.

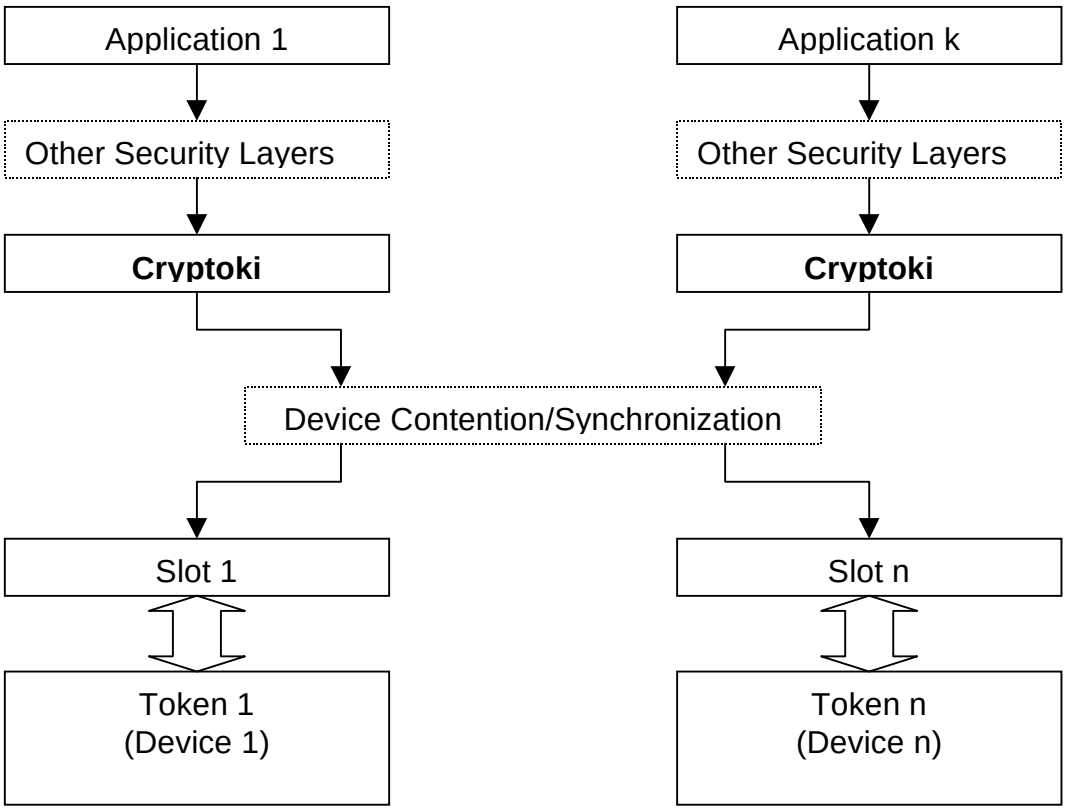
۱۰-۲ دستورالعمل ارزیابی توکن‌های امنیتی جهت استفاده در زیرساخت کلید عمومی کشور

دستورالعمل ارزیابی توکن‌های امنیتی یک دستورالعمل اجرایی جهت ارزیابی توکن‌های امنیتی بر اساس استاندارد ملزومات امنیتی توکن‌های سخت‌افزاری می‌باشد. آزمایشگاه‌های ارزیابی نرم‌افزارهای PKE و توکن‌های امنیتی موظف هستند که منطبق با این دستورالعمل اجرایی، برنامه ارزیابی خود را طراحی و اعمال نمایند.

در دستورالعمل اجرایی ارزیابی توکن‌های امنیتی می‌بایست روش اجرایی ارزیابی توکن‌های امنیتی بر اساس ملزومات بیان شده در استاندارد ملزومات امنیتی توکن‌های سخت‌افزاری در هر یک از حوزه‌های نام برده شده در این استاندارد، تشریح گردد. همچنین نحوه تخمین سطح امنیتی توکن ارزیابی شده بر اساس سطوح امنیتی تخمین زده شده در هر حوزه، می‌بایست مشخص گردد.

۱۰-۳ ملزومات واسط‌های نرم‌افزاری جهت مدیریت ماژول‌های سخت‌افزاری رمزنگاری

برقراری ارتباط نرم‌افزارهای مختلف با هر ماژول سخت‌افزاری رمزنگاری از طریق یک واسط نرم‌افزاری امکان‌پذیر می‌باشد؛ بدین ترتیب که نرم‌افزار مورد نظر واسط نرم‌افزاری را بارگذاری نموده و با فراخوانی توابع این واسط، عملیات کنترلی و رمزنگاری مختلف را از طریق ماژول رمزنگاری انجام می‌دهد. بعنوان مثال چنانچه توکن امنیتی از واسط استاندارد PKCS#11 پشتیبانی نماید، مطابق با شکل ذیل نرم‌افزارهای مختلف با بارگذاری واسط Cryptoki و فراخوانی توابع این واسط، با توکن‌های امنیتی ارتباط برقرار می‌نمایند. هر Slot معادل با یک واسط فیزیکی می‌باشد که توکن از طریق این واسط به سیستم متصل می‌شود.



در واسط نرم‌افزاری مورد استفاده جهت مدیریت ماژول‌های سخت‌افزاری رمزنگاری می‌بایست ملزومات امنیتی مختلف از جمله قابلیت تعریف نقش‌های مختلف و هویت شناسی این نقش‌ها، کنترل دسترسی به واحدهای اطلاعاتی دخیره شده در ماژول و امکان امحای اطلاعات و راه‌اندازی اولیه ماژول اعمال شده باشد.

در استاندارد واسط‌های نرم‌افزاری، واسط‌های نرم‌افزاری مناسب و پذیرفته شده جهت مدیریت ماژول‌های سخت-افزاری رمزنگاری مورد استفاده در زیرساخت کلید عمومی کشور از جمله توکن‌های امنیتی و ماژول‌های HSM بسته به کارایی و نوع کاربرد، معرفی می‌گردد.

۱۱ تجهیز برنامه‌های کاربردی به زیرساخت کلید عمومی

۱۱-۱ ملزومات برنامه‌های کاربردی مجهز به زیرساخت کلید عمومی

سیستم‌های رمزنگاری کلید عمومی، جهت ایجاد امنیت در تبادل اطلاعات با فراهم آوردن سرویس‌های امنیتی مختلف از قبیل اطمینان از جامعیت یا دست‌نخوردگی و حفظ محرمانگی اطلاعات، احراز هویت موجودیت‌ها، انکارناپذیری و کنترل دسترسی به منابع اطلاعاتی طراحی شده‌اند.

به فرآیند تجهیز برنامه‌های کاربردی به استفاده از گواهینامه‌های دیجیتالی برای پیاده‌سازی سرویس‌های فوق، تجهیز برنامه کاربردی به زیرساخت کلید عمومی (PK-Enabling) گفته می‌شود. به برنامه‌های کاربردی که از زیرساخت کلید عمومی (PKI) استفاده می‌نمایند، برنامه‌های کاربردی مجهز به به زیرساخت کلید عمومی (PK-Enabled که به اختصار PKE معرفی می‌گردند) گفته می‌شود.

تجهیز یک برنامه کاربردی و یا سیستم اطلاعاتی به زیرساخت کلید عمومی قابلیت‌های امنیتی مختلفی را به همراه دارد، برخی از این قابلیت‌ها و کاربردها در ذیل خلاصه شده‌اند:

- انکارناپذیری تراکنش‌های انجام شده توسط کاربران در یک برنامه کاربردی و یا سیستم اطلاعاتی؛
- احراز هویت کاربران بصورت دوعامله و از طریق توکن سخت‌افزاری؛
- اعمال کنترل دسترسی و مجوزدهی به کاربران جهت دسترسی به منابع اطلاعاتی مختلف و عملیات اجرایی؛
- امن‌سازی ترافیک شبکه از طریق پروتکل‌های امنیتی مبتنی بر زیرساخت کلید عمومی (احراز هویت و حفظ محرمانگی در حین انتقال اطلاعات)؛
- حفظ محرمانگی اطلاعات در زمان ذخیره‌سازی؛
- اطمینان از جامعیت و اصالت منابع اطلاعاتی و کدهای اجرایی نظیر ActiveX و Applet؛
- پست الکترونیک امن (امضای دیجیتال و رمزگذاری نامه‌ها)؛
- ایجاد شبکه‌های خصوصی مجازی (VPN)

در استانداردهای امنیتی مختلف از جمله استانداردهای منتشر شده توسط DOD ، ملزومات برنامه‌های کاربردی PKE تعیین شده است که این ملزومات می‌بایست در مرحله تجهیز برنامه کابردی به زیرساخت کلید عمومی و تدوین دستورالعمل اجرایی ارزیابی نرم‌افزارهای PKE در نظر گرفته شود. با توجه به اهمیت و لزوم اعمال فرآیند تجهیز برنامه‌های کاربردی حساس و با اهمیت به زیرساخت کلید عمومی کشور و لزوم راه‌اندازی آزمایشگاه‌های ارزیابی نرم‌افزارهای PKE ، وجود یک استاندارد بومی جهت تشریح فرآیند PK-Enabling و تعیین ملزومات لازم برای نرم‌افزارهای مجهز به زیرساخت کلید کشور، کاملاً ضروری به نظر می‌رسد. این استاندارد می‌بایست ملزومات نرم‌افزارهای PKE را در حوزه‌های مختلفی از جمله ماژول‌های رمزنگاری، امنیت کامپیوتر، مدیریت کلید، پروتکل-

های ارتباطی، درخواست و دریافت گواهی جدید برای صاحبان امضا، دریافت گواهی و CRL برای طرف‌های اعتماد کننده، بررسی وضعیت ابطال یا عدم ابطال گواهی‌ها، تشکیل و اعتبارسنجی زنجیره گواهی، الگوریتم‌های رمزنگاری و پیکربندی و مستندسازی نرم‌افزار PKE ، تشریح نماید.

۱۱-۲ دستورالعمل ارزیابی برنامه‌های کاربردی مجهز به زیرساخت کلید عمومی

دستورالعمل ارزیابی برنامه‌های کاربردی PKE، یک دستورالعمل اجرایی جهت ارزیابی نرم‌افزارهای PKE بر اساس استاندارد ملزومات برنامه‌های کاربردی مجهز شده به زیرساخت کلید عمومی، می‌باشد. آزمایشگاه‌های ارزیابی نرم-افزارهای PKE موظف هستند که منطبق با این دستورالعمل اجرایی، برنامه ارزیابی خود را طراحی و اعمال نمایند.

در دستورالعمل اجرایی ارزیابی برنامه‌های کاربردی مجهز شده به زیرساخت کلید عمومی، می‌بایست روش اجرایی ارزیابی برنامه‌های کاربردی PKE بر اساس ملزومات بیان شده در استاندارد ملزومات برنامه‌های کاربردی مجهز شده به زیرساخت کلید عمومی، در هر یک از حوزه‌های نام برده شده در این استاندارد، تشریح گردد. همچنین نحوه تخمین سطح امنیتی نرم‌افزار ارزیابی شده بر اساس سطوح امنیتی تخمین زده شده در هر حوزه، می‌بایست مشخص گردد.

۱۲ موارد دیگر

۱۲-۱ ملزومات تدوین سیاست‌ها و دستورالعمل‌های اجرایی مراکز صدور گواهی

سیاست‌های گواهی الکترونیکی (CP) یک مرکز صدور گواهی به معنی ملزومات در نظر گرفته شده برای این مرکز جهت صدور و مدیریت گواهی‌های الکترونیکی می‌باشد که در دستورالعمل اجرایی مراکز صدور گواهی الکترونیکی (CPS)، شیوه‌ها و چگونگی اعمال این ملزومات جهت فراهم نمودن خدمات گواهی‌های الکترونیکی از قبیل صدور و ابطال گواهی‌ها، مدیریت و تجدید کلید و اعلام وضعیت ابطال یا عدم ابطال گواهی‌ها، تشریح می‌گردد.

تدوین سیاست‌ها و دستورالعمل‌های اجرایی مراکز صدور گواهی کشور می‌بایست منطبق با ساختار ارائه شده در RFC 3647 صورت گیرد.

۱۲-۲ ملزومات رمزنگاری مبتنی بر کلمه عبور

در این استاندارد روش رمزنگاری متقارن اطلاعات با استفاده از کلید سری استخراج شده از یک کلمه عبور، تشریح می‌گردد. این روش بطور معمول جهت رمزگذاری کلید خصوصی به منظور انتقال آن از یک سیستم به سیستم دیگر

مورد استفاده قرار می‌گیرد. در زیرساخت کلید عمومی کشور، رمزگذاری مبتنی بر کلمه عبور می‌بایست منطبق با استاندارد PKCS#5 صورت گیرد.

۱۲-۳ ملزومات ساختار پیام‌های رمزنگاری (CMS)[1]

در این استاندارد به منظور ایجاد یکپارچگی و هماهنگی بین نرم‌افزارهای PKE مختلف، یک ساختار کلی برای اطلاعات رمزنگاری از جمله اطلاعات امضا شده و یا رمزگذاری شده تعریف می‌گردد؛ بدین ترتیب‌که در آن انواع مختلف داده‌ای از قبیل data، Signed data، enveloped data، signed-and-enveloped-data و digested data تعریف شده است که ساختار اطلاعات رمزنگاری مختلف، بر اساس این انواع شکل می‌گیرد. بعنوان مثال جهت تعریف مجموعه‌ای از گواهی‌های الکترونیکی موجود در یک زنجیره گواهی و یا مجموعه‌ای از لیست گواهی باطل شده در یک ساختار واحد، می‌بایست این اطلاعات در قالب استاندارد CMS و منطبق با نوع داده‌ای Signed-data، کدگذاری گردند.

بنابراین در زیرساخت کلید عمومی کشور وجود یک استاندارد ملی برای تعریف ساختار پیام‌های رمزنگاری منطبق با استاندارد PKCS#7 لازم و ضروری می‌باشد.

۱۲-۴ ملزومات ساختار اطلاعات مربوط به کلید خصوصی

استاندارد PKCS#8 یک ساختار برای اطلاعات کلید خصوصی متناظر با کلید عمومی و کلید خصوصی رمزگذاری شده تعریف می‌نماید. در این استاندارد کلید خصوصی با استفاده از یک روش رمزگذاری مبتنی بر کلمه عبور و منطبق با استاندارد PKCS#5 رمزگذاری می‌گردد. چنانچه در یک نرم‌افزار نیاز باشد که کلید خصوصی بصورت مستقل و در قالب یک فایل بارگذاری گردد و یا مورد استفاده قرار گیرد، این فایل می‌بایست منطبق با استاندارد PKCS#8 در فرمت رمزگذاری شده، ایجاد گردد.

۱۲-۵ ملزومات ساختار تبادل اطلاعات شخصی

استاندارد PKCS#12 یک ساختار برای تبادل اطلاعات شناسایی شخصی شامل کلید خصوصی، مجموعه‌ای از گواهی‌های الکترونیکی و اطلاعات شخصی دیگرتعریف می‌نماید. در PKCS#12 به استانداردهای دیگری از جمله PKCS#5، PKCS#7 و PKCS#8 نیز ارجاع داده شده است. این استاندارد از انتقال مستقیم اطلاعات شخصی تحت چندین مد امنیتی محرمانگی و تمامیت، پشتیبانی می‌نماید. در زیر ساخت کلید عمومی کشور چنانچه نیاز به انتقال کلید خصوصی و گواهی‌های الکترونیکی از طریق فایل باشد، این فایل می‌بایست در قالب استاندارد PKCS#12 بطوریکه در آن حداقل از مد محرمانگی و تمامیت مبتنی بر کلمه عبور پشتیبانی شده باشد، تولید گردد.

[1] Cryptographic Message Syntax