ردیف	عنوان انگلیسی	عنوان فارسی
1	INTRODUCTION	مقدمه
1.1	Overview	خلاصه
1.2	Document name and identification	نام و شناسه سند
1.3	PKI participants	اجزاء زیرساخت کلید عمومی
1.3.1	Certification authorities	مراکز صدور گواهی الکترونیکی
1.3.2	Registration authorities	دفاتر ثبت نام
1.3.3	Subscribers	صاحبان امضاء
1.3.4	Relying parties	طرف های اعتماد کننده
1.3.5	Other participants	اجزاء دیگر
1.4	Certificate usage	کاربردهای گواهی
1.4.1.	Appropriate certificate uses	مصارف مناسب گواهی
1.4.2	Prohibited certificate uses	مصارف غیر مجاز گواهی
1.5	Policy administration	راهبری سیاست ها
1.5.1	Organization administering the document	سازمان راهبری سند
1.5.2	Contact person	اطلاعات تماس
1.5.3	Person determining CPS suitability for the policy	مسئول تطبیق دستورالعمل اجرایی با سیاست های مرکز
1.5.4	CPS approval procedures	رویه تایید دستورالعمل اجرایی
1.6	Definitions and acronyms	تعاریف و اختصارات
2	PUBLICATION AND REPOSITORY RESPONSIBILITIE	انتشار و وظایف مخزن
2.1	Repositories	مخزن
2.2	Publication of certification information	انتشار اطلاعات گواهی
2.3	Time or frequency of publication	زمان یا تناوب انتشار
2.4	Access controls on repositories	کنترل دسترسی روی مخازن
3	(11)IDENTIFICATION AND AUTHENTICATION	شناسایی و احراز هویت

نام گذاری	Naming	3.1
انواع نام ها	Types of names	3.1.1
نیاز به نام های با معنی	Need for names to be meaningful	3.1.2
استفاده از نام های مستعار غیر واقعی برای صاحبان امضا	Anonymity or pseudonymity of subscribers	3.1.3
قواعد تفسیر قالب های مختلف نام ها	Rules for interpreting various name forms	3.1.4
یکتایی نام ها	Uniqueness of names	3.1.5
تشخیص، احراز هویت و نقش نام های تجاری	Recognition, authentication, and role of trademarks	3.1.6
تایید شناسایی اولیه	Initial identity validation	3.2
روش اثبات تصرف (مالکیت)کلید خصوصی	Method to prove possession of private key	3.2.1
احراز هویت سازمان ها	Authentication of organization identity	3.2.2
احراز هویت افراد	Authentication of individual identity	3.2.3
اطلاعات تصدیق نشده صاحبان امضاء	Non-verified subscriber information	3.2.4
اعتبارسنجی مرجع ذیصلاح	Validation of authority	3.2.5
معیارهای همکاری با سایر مراکز	Criteria for interoperation	3.2.6
شناسایی و احراز هویت برای درخواست‌های تجدید کلید	Identification and authentication for re-key requests	3.3
روال شناسایی و احراز هویت برای تجدید کلید (عادی)	Identification and authentication for routine re-key	3.3.1
شناسایی و احراز هویت برای تجدید کلید پس از ابطال گواهی	Identification and authentication for re-key after revocation	3.3.2
شناسایی و احراز هویت برای درخواست ابطال	Identification and authentication for revocation request	3.4
نیازهای عملیاتی در چرخه حیات گواهی	**(11)CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS**	**4**
درخواست گواهی	Certificate Application	4.1
موجودیت های مجاز برای ارائه درخواست گواهی	Who can submit a certificate application	4.1.1
فرایند ثبت نام و مسئولیت ها	Enrollment process and responsibilities	4.1.2
فرایند درخواست گواهی	Certificate application processing	4.2
اجرای فرایند شناسایی و احراز هویت	Performing identification and authentication functions	4.2.1
تایید یا عدم تایید درخواست های گواهی	Approval or rejection of certificate applications	4.2.2
مدت فرایند رسیدگی به درخواست گواهی	Time to process certificate applications	4.2.3
صدور گواهی	Certificate issuance	4.3
اقدامات مرکز در طول صدور گواهی	CA actions during certificate issuance	4.3.1

4.3.2	Notification to subscriber by the CA of issuance of certificate	اطلاع رسانی به صاحب امضاء توسط مرکز
4.4	Certificate acceptance	پذیرش گواهی
4.4.1	Conduct constituting certificate acceptance	روال پذیرش گواهی
4.4.2	Publication of the certificate by the CA	انتشار گواهی توسط مرکز صدور گواهی
4.4.3	Notification of certificate issuance by the CA to other entities	اطلاع رسانی صدور گواهی به سایر موجودیت ها توسط مرکز
4.5	Key pair and certificate usage	کاربرد گواهی و زوج کلید
4.5.1	Subscriber private key and certificate usage	کاربرد گواهی و کلید خصوصی صاحب امضاء
4.5.2	Relying party public key and certificate usage	کاربرد گواهی و کلید عمومی برای طرف اعتماد کننده
4.6	Certificate renewal	تمدید گواهی
4.6.1	Circumstance for certificate renewal	شرایط تمدید گواهی
4.6.2	Who may request renewal	متقاضیان تمدید گواهی
4.6.3	Processing certificate renewal requests	روال رسیدگی به درخواست های تمدید گواهی
4.6.4	Notification of new certificate issuance to subscriber	اعلام صدور گواهی به صاحب امضاء
4.6.5	Conduct constituting acceptance of a renewal certificate	روال پذیرش گواهی تمدید شده
4.6.6	Publication of the renewal certificate by the CA	انتشار گواهی های تمدید شده توسط مرکز
4.6.7	Notification of certificate issuance by the CA to other entities	اطلاع رسانی صدور گواهی توسط مرکز به موجودیت‌های دیگر
4.7	Certificate re-key	تجدید کلید گواهی
4.7.1	Circumstance for certificate re-key	شرایط تجدید کلید گواهی
4.7.2	Who may request certification of a new public key	متقاضیان گواهی با کلید عمومی جدید
4.7.3	Processing certificate re-keying requests	فرایند رسیدگی به درخواست های تجدید کلید گواهی
4.7.4	Notification of new certificate issuance to subscriber	اعلام صدور گواهی جدید به صاحب امضاء
4.7.5	Conduct constituting acceptance of a re-keyed certificate	روال پذیرش گواهی با کلید جدید
4.7.6	Publication of the re-keyed certificate by the CA	انتشار گوا هی تجدید کلید شده توسط مرکز
4.7.7	Notification of certificate issuance by the CA to other entities	اطلاع رسانی صدور گواهی توسط مرکز به موجودیت‌های دیگر
4.8	Certificate modification	اصلاح گواهی
4.8.1	Circumstance for certificate modification	شرایط اصلاح گواهی
4.8.2	Who may request certificate modification	متقاضیان درخواست اصلاح گواهی
4.8.3	Processing certificate modification requests	فرایند رسیدگی به درخواست های اصلاح گواهی

اعلام صدور گواهی جدید به صاحب امضاء	Notification of new certificate issuance to subscriber	4.8.4
روال پذیرش گواهی اصلاح شده	Conduct constituting acceptance of modified certificate	4.8.5
انتشار گواهی اصلاح شده توسط مرکز	Publication of the modified certificate by the CA	4.8.6
اطلاع رسانی صدور گواهی توسط مرکز به موجودیت‌های دیگر	Notification of certificate issuance by the CA to other entities	4.8.7
ابطال و تعلیق گواهی	Certificate revocation and suspension	4.9
شرایط ابطال	Circumstances for revocation	4.9.1
افرادی که می توانند درخواست ابطال نمایند	Who can request revocation	4.9.2
روال رسیدگی به درخواست ابطال	Procedure for revocation request	4.9.3
مهلت اعلام درخواست ابطال	Revocation request grace period	4.9.4
مدت رسیدگی به درخواست ابطال توسط مرکز	Time within which CA must process the revocation request	4.9.5
الزام کنترل ابطال توسط طرف های اعتماد کننده	Revocation checking requirement for relying parties	4.9.6
تناوب صدور لیست گواهی های باطل شده	(if applicable)CRL issuance frequency	4.9.7
حداکثر تاخیر انتشار لیست گواهی های باطل شده	(if applicable)Maximum latency for CRLs	4.9.8
امکان کنترل برخط وضعیت یا ابطال	On-line revocation/status checking availability	4.9.9
ملزومات کنترل برخط وضعیت یا ابطال	On-line revocation checking requirements	4.9.10
سایر روش های ممکن اعلان ابطال	Other forms of revocation advertisements available	4.9.11
الزامات خاص در صورت افشای کلید	Special requirements re-key compromise	4.9.12
شرایط تعلیق	Circumstances for suspension	4.9.13
کسانی که می توانند درخواست تعلیق نمایند	Who can request suspension	4.9.14
روال رسیدگی به درخواست تعلیق	Procedure for suspension request	4.9.15
محدودیت های دوره تعلیق	Limits on suspension period	4.9.16
خدمات وضعیت گواهی	Certificate status services	4.1
ویژگی های عملیاتی	Operational characteristics	4.10.1
دسترس پذیری خدمت (سرویس)	Service availability	4.10.2
ویژگی های اختیاری	Optional features	4.10.3
پایان اشتراک	End of subscription	4.11
امانتگذاری و بازیابی کلید	Key escrow and recovery	4.12
سیاست ها و دستورالعمل اجرایی امانتگذاری و بازیابی کلید	Key escrow and recovery policy and practices	4.12.1

سیاست ها و دستورالعمل اجرایی بازیابی و اطلاعات مورد نیاز دسترسی به کلید	Session key encapsulation and recovery policy and practices	4.12.2
کنترل های عملیاتی، مدیریتی و تجهیزاتی	**(11)FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS**	**5**
کنترل های فیزیکی	Physical controls	5.1
ساختمان و مکان سایت	Site location and construction	5.1.1
دسترسی فیزیکی	Physical access	5.1.2
تهویه هوا و منبع تغذیه برق	Power and air conditioning	5.1.3
جلوگیری از آب گرفتگی	Water exposures	5.1.4
پیش گیری و محافظت در مقابل آتش	Fire prevention and protection	5.1.5
نگهداری سخت افزار ذخیره سازی	Media storage	5.1.6
انهدام سخت افزار ذخیره سازی بدون استفاده	Waste disposal	5.1.7
نسخه پشتیبان خارج از سایت	Off-site backup	5.1.8
کنترل های رویه ای	Procedural controls	5.2
نقش های مورد اطمینان	Trusted roles	5.2.1
تعداد افراد مورد نیاز برای هر نقش	Number of persons required per task	5.2.2
شناسایی و احراز هویت برای هر نقش	Identification and authentication for each role	5.2.3
نقش ها با وظایف مجزا	Roles requiring separation of duties	5.2.4
کنترل کارکنان	Personnel controls	5.3
ملزومات مربوط به قابلیت ها، سابقه و عدم سوء پیشینه	Qualifications, experience, and clearance requirements	5.3.1
رویه بررسی سابقه افراد	Background check procedures	5.3.2
نیازمندی های آموزشی	Training requirements	5.3.3
بسامد و نیازهای بازآموزی	Retraining frequency and requirements	5.3.4
دوره زمانی و ترتیب چرخش کار	Job rotation frequency and sequence	5.3.5
جریمه های اقدامات خارج از محدوده اختیارات	Sanctions for unauthorized actions	5.3.6
الزامات پیمانکاران مستقل	Independent contractor requirements	5.3.7
مستندات فراهم شده برای کارکنان	Documentation supplied to personnel	5.3.8
روال های ثبت رویدادهای بازرسی امنیتی	Audit logging procedures	5.4
انواع رویدادهای قابل ثبت	Types of events recorded	5.4.1
تناوب پردازش اطلاعات رویدادهای ثبت شده	Frequency of processing log	5.4.2

5.4.3	Retention period for audit log	دوره نگهداری از اطلاعات رویدادهای ثبت شده
5.4.4	Protection of audit log	محافظت از اطلاعات رویدادهای ثبت شده
5.4.5	Audit log backup procedures	روال های تهیه نسخه پشتیبان از اطلاعات بازرسی امنیتی
5.4.6	(internal vs. external)Audit collection system	سامانه جمع آوری اطلاعات بازرسی امنیتی
5.4.7	Notification to event-causing subject	تذکر به مسبب رویداد
5.4.8	Vulnerability assessments	ارزیابی آسیب پذیری
5.5	Records archival	بایگانی اطلاعات
5.5.1	Types of records archived	انواع اطلاعات بایگانی شده
5.5.2	Retention period for archive	دوره نگهداری اطلاعات بایگانی شده
5.5.3	Protection of archive	محافظت از بایگانی
5.5.4	Archive backup procedures	روال های تهیه نسخه پشتیبان از بایگانی
5.5.5	Requirements for time-stamping of records	الزامات مهر زمانی اطلاعات بایگانی
5.5.6	(internal or external)Archive collection system	سامانه جمع آوری بایگانی
5.5.7	Procedures to obtain and verify archive information	روال های بدست آوردن و بررسی اطلاعات بایگانی
5.6	Key changeover	گردش کلید
5.7	Compromise and disaster recovery	بازیابی به علت سوانح غیر مترقبه و در خطر افشاء بودن
5.7.1	Incident and compromise handling procedures	روال های مقابله با افشاء کلید و حوادث
5.7.2	Computing resources, software, and/or data are corrupted	از بین رفتن تجهیزات کامپیوتری، نرم افزار و داده ها
5.7.3	Entity private key compromise procedures	رویه های در خطر افشاء قرار گرفتن کلید خصوصی موجودیت
5.7.4	Business continuity capabilities after a disaster	ادامه فعالیت های اصلی بعد از وقوع حوادث
5.8	CA or RA termination	پایان فعالیت مرکز صدور گواهی یا دفتر ثبت نام
6	**(11)TECHNICAL SECURITY CONTROLS**	**کنترل های امنیتی فنی**
6.1	Key pair generation and installation	تولید و نصب زوج کلید
6.1.1	Key pair generation	تولید زوج کلید
6.1.2	Private key delivery to subscriber	تحویل کلید خصوصی به صاحب امضاء
6.1.3	Public key delivery to certificate issuer	تحویل کلید عمومی به مرکز صدور گواهی الکترونیکی
6.1.4	CA public key delivery to relying parties	تحویل کلید عمومی مرکز صدور گواهی به طرف های اعتماد کننده
6.1.5	Key sizes	طول کلید

6.1.6	Public key parameters generation and quality checking	تولید پارامترهای کلید عمومی و کنترل کیفیت
6.1.7	(as per X.509 v3 key usage field)Key usage purposes	موارد کاربرد کلید (طبق فیلد کاربرد کلید X.۵۰۹ V۳)
6.2	Private Key Protection and Cryptographic Module Engineering Controls	محافظت از کلیدهای خصوصی و کنترل های مهندسی دستگاه های رمزنگاری
6.2.1	Cryptographic module standards and controls	کنترل ها و استانداردهای ماژول های رمزنگاری
6.2.2	Private key (n out of m) multi-person control	کنترل چند نفره (n از m) به کلید خصوصی
6.2.3	Private key escrow	دستیابی قانونی به کلید خصوصی
6.2.4	Private key backup	تهیه نسخه پشتیبان از کلید خصوصی
6.2.5	Private key archival	بایگانی کلید خصوصی
6.2.6	Private key transfer into or from a cryptographic module	انتقال کلید خصوصی به یا از یک دستگاه رمزنگاری
6.2.7	Private key storage on cryptographic module	ذخیره سازی کلیدهای خصوصی در دستگاه رمزنگاری
6.2.8	Method of activating private key	روش فعال سازی کلید خصوصی
6.2.9	Method of deactivating private key	روش غیرفعال نمودن کلید خصوصی
6.2.10	Method of destroying private key	روش نابود کردن کلید خصوصی
6.2.11	Cryptographic Module Rating	درجه بندی دستگاه رمزنگاری
6.3	Other aspects of key pair management	وجوه دیگر مدیریت زوج کلید
6.3.1	Public key archival	بایگانی کلید عمومی
6.3.2	Certificate operational periods and key pair usage periods	دوره های عملیاتی گواهی و دوره‌های استفاده از زوج کلید
6.4	Activation data	اطلاعات فعال ساز
6.4.1	Activation data generation and installation	تولید و به کارگیری اطلاعات فعال ساز
6.4.2	Activation data protection	محافظت از اطلاعات فعال ساز
6.4.3	Other aspects of activation data	وجوه دیگر اطلاعات فعال ساز
6.5	Computer security controls	کنترل های امنیتی رایانه
6.5.1	Specific computer security technical requirements	نیازهای خاص فنی امنیتی رایانه
6.5.2	Computer security rating	درجه بندی امنیتی رایانه
6.6	Life cycle technical controls	کنترل های فنی طول عمر
6.6.1	System development controls	کنترلهای توسعه سیستم
6.6.2	Security management controls	کنترل های مدیریتی امنیت
6.6.3	Life cycle security controls	کنترل های امنیتی طول عمر

کنترل های امنیتی شبکه	Network security controls	6.7
مهر زمانی	Time-stamping	6.8
مشخصات گواهی، CRL و OCSP	**CERTIFICATE, CRL, AND OCSP PROFILES**	**7**
مشخصات گواهی	Certificate profile	7.1
شماره نسخه	(s)Version number	7.1.1
ملحقات گواهی	Certificate extensions	7.1.2
شناسه الگوریتم ها	Algorithm object identifiers	7.1.3
قالب نام ها	Name forms	7.1.4
محدودیت در نام گذاری	Name constraints	7.1.5
شناسه سیاست های گواهی	Certificate policy object identifier	7.1.6
کاربرد فیلد الحاقی Policy Constraints	Usage of Policy Constraints extension	7.1.7
ساختار توصیف کننده سیاست و معنای آن	Policy qualifiers syntax and semantics	7.1.8
پردازش معنایی برای فیلد الحاقی حیاتی Certificate Policies	Processing semantics for the critical Certificate Policies extension	7.1.9
مشخصات لیست گواهی های باطل شده	CRL profile	7.2
شماره نسخه	(s)Version number	7.2.1
ملحقات CRL و CRL Entry	CRL and CRL entry extensions	7.2.2
مشخصات OCSP	OCSP profile	7.3
شماره نسخه	(s)Version number	7.3.1
ملحقات OCSP	OCSP extensions	7.3.2
بازرسی تطابق و سایر ارزیابی های دیگر	**COMPLIANCE AUDIT AND OTHER ASSESSMENTS**	**8**
تناوب و شرایط ارزیابی	Frequency or circumstances of assessment	8.1
هویت و صلاحیت بازرس	Identity/qualifications of assessor	8.2
ارتباط بازرس با مرکز ارزیابی شونده	Assessor's relationship to assessed entity	8.3
موضوعات مورد ارزیابی	Topics covered by assessment	8.4
اقدامات اتخاذ شده در برخورد با نقایص	Actions taken as a result of deficiency	8.5
گزارش نتایج	Communication of results	8.6
سایر موضوعات حقوقی و مربوط به کسب و کار	**OTHER BUSINESS AND LEGAL MATTERS**	**9**
تعرفه ها	Fees	9.1

9.1.1	Certificate issuance or renewal fees	تعرفه های صدور گواهی یا تمدید گواهی
9.1.2	Certificate access fees	تعرفه های دسترسی به اطلاعات گواهی
9.1.3	Revocation or status information access fees	تعرفه های ابطال یا دسترسی به ابطال وضعیت گواهی
9.1.4	Fees for other services	تعرفه سایر خدمات
9.1.5	Refund policy	سیاست استرداد
9.2	Financial responsibility	تعهدات مالی
9.2.1	Insurance coverage	پوشش بیمه ای
9.2.2	Other assets	سایر دارایی های
9.2.3	Insurance or warranty coverage for end-entities	پوشش بیمه ای و گارانتی برای موجودیت های نهایی
9.3	Confidentiality of business information	محرمانگی اطلاعات مربوط به کسب و کار
9.3.1	Scope of confidential information	محدوده اطلاعات محرمانه
9.3.2	Information not within the scope of confidential information	اطلاعات که در محدوده اطلاعات محرمانه نمی باشند
9.3.3	Responsibility to protect confidential information	مسئولیت محافظت از محرمانگی اطلاعات
9.4	Privacy of personal information	محافظت از اطلاعات شخصی
9.4.1	Privacy plan	طرح حریم خصوصی
9.4.2	Information treated as private	اطلاعاتی که خصوصی محسوب می شوند
9.4.3	Information not deemed private	اطلاعاتی که خصوصی محسوب نمی شوند
9.4.4	Responsibility to protect private information	مسئولیت محافظت از اطلاعات شخصی
9.4.5	Notice and consent to use private information	آگاهی و رضایت برای استفاده از اطلاعات خصوصی
9.4.6	Disclosure pursuant to judicial or administrative process	افشا مطابق با فرآیندهای اداری و قضایی
9.4.7	Other information disclosure circumstances	سایر شرایط افشای اطلاعات
9.5	Intellectual property rights	حق مالکیت معنوی
9.5.1		حق مالکیت معنوی گواهی و اطلاعات ابطال گواهی
9.5.2		حق مالکیت معنوی CPS
9.5.3		حق مالکیت معنوی نامها
9.5.4		حق مالکیت معنوی کلیدها
9.6	Representations and warranties	مسئولیت ها و التزامات
9.6.1	CA representations and warranties	مسئولیت ها و التزامات مرکز میانی

مسئولیت ها و التزامات دفاتر ثبت نام	RA representations and warranties	9.6.2
مسئولیت ها و التزامات صاحبان امضاء	Subscriber representations and warranties	9.6.3
مسئولیت ها و التزامات طرف های اعتماد کننده	Relying party representations and warranties	9.6.4
مسئولیت ها و التزامات موجودیت های دیگر	Representations and warranties of other participants	9.6.5
عدم پذیرش ضمانت ها	Disclaimers of warranties	9.7
محدودیت مسئولیت ها	Limitations of liability	9.8
خسارت ها	Indemnities	9.9
دوره و خاتمه	Term and termination	9.1
دوره	Term	9.10.1
خاتمه	Termination	9.10.2
اثرات خاتمه و ابقاء	Effect of termination and survival	9.10.3
اخطارهای فردی و ارتباطات با موجودیت های	Individual notices and communications with participants	9.11
تغییرات	Amendments	9.12
روال تغییر	Procedure for amendment	9.12.1
مکانیزم و دوره اطلاع رسانی	Notification mechanism and period	9.12.2
شرایط تغییر OID	Circumstances under which OID must be changed	9.12.3
روال های حل اختلاف	Dispute resolution provisions	9.13
قوانین حاکم	Governing law	9.14
تطابق با قوانین اجرایی	Compliance with applicable law	9.15
الزامات متفرقه	Miscellaneous provisions	9.16
توافقنامه کلی	Entire agreement	9.16.1
تخصیص	Assignment	9.16.2
عدم وابستگی	Severability	9.16.3
اجرای تعرفه های وکالت و فسخ مالکیت	(attorneys' fees and waiver of rights)Enforcement	9.16.4
فورس ماژور	Force Majeure	9.16.5
سایر قیود	Other provisions	9.17