



امنیت تجارت الکترونیک

مؤلفین:

امیرحسین حسن زاده نفه‌تن - مهدی اسدیک - ابراهیم اسدزاده



www.ketab.ir



سرشناسه	: حسن زاده نفوتی، امیرحسین، ۱۳۷۳-
عنوان و نام پدیدآور	: امنیت تجارت الکترونیک/مؤلفین امیرحسین حسن زاده نفوتی، مهدی اسدبک، ابراهیم اسدزاده.
مشخصات نشر	: تهران: زلال سبز، ۱۳۹۹.
مشخصات ظاهری	: ۱۸۹ ص.: مصور، جدول، نمودار.
شابک	: ۹۷۸-۶۲۲-۷۲۸۹۳۷-۴
وضعیت فهرست نویسی	: فیا
یادداشت	: کتابنامه.
موضوع	: بازرگانی الکترونیکی -- تدابیر امنیتی
موضوع	: Electronic commerce -- Security measures
موضوع	: بانک و بانکداری -- تدابیر امنیتی
موضوع	: Banks and banking -- Security measures
شناسه افزوده	: اسدزاده، ابراهیم، ۱۳۵۸ -
شناسه آهوده	: اسدبک، مهدی، ۱۳۷۳-
شناسه آهوده	: Asadbak, Mehdi
رده بندی کنگره	: HF۵۵۲۸/۳۳
رده بندی دیوبند	: ۶۵۸/۸۴
شماره کتابخانه ملی	: ۷۳۰۶۱۲۶

تهران: میدان بلاغ، باز: بزرگ کتاب، واحد ۲۲. نشر و پخش همراه ۰۹۱۲۲۳۷۴۷۱۵-۰۶۶۴۸۰۴۶۸-

عنوان: امنیت تجارت الکترونیک

نویسندگان: امیرحسین حسن زاده نفوتی، مهدی اسدبک، ابراهیم اسدزاده

صفحه آرای و طراحی جلد: امیرحسین حسن زاده نفوتی

ویرایش: شورای بررسی موسسه انتشاراتی زلال سبز

نشر و پخش: موسسه فرهنگی انتشاراتی زلال سبز

نوبت چاپ: اول، ۱۳۹۹

شمارگان: ۱۰۰۰ نسخه

چاپ: سورنا

قیمت: ۴۵۰۰ تومان

شابک: ۹۷۸-۶۲۲-۷۲۸۹-۳۷-۴

امروزه فناوری اطلاعات و ارتباطات محور توسعه اقتصادی، اجتماعی و فرهنگی کشورهای مختلف قرار گرفته است. تجارت الکترونیکی یکی از نموده‌های عینی انقلاب فناوری اطلاعات و ارتباطات در عرصه‌های اقتصادی است. ظهور اینترنت و تجاری شدن آن در دهه‌های اخیر شیوه‌های سنتی تجارت را متحول نموده است. تجارت الکترونیکی انقلابی در شیوه‌ها و رویه‌های تجاری گذشته ایجاد کرده و سرعت و صرفه‌جویی را در بهترین وجه جامه عمل پوشانده است. در محیط الکترونیکی فاصله‌های جغرافیایی و محدودیت‌های زمانی و مکانی منتفی و مبادلات تجاری بر پایه اطلاعات الکترونیکی انجام می‌شود. تجارت الکترونیکی با رفع موانع فراروی تجارت بین‌الملل روند تجارت جهانی را تسریع می‌نماید. تجارت الکترونیکی از مزایا و پیامدهای اقتصادی مهمی از قبیل گسترش بازار، کاهش قیمت منابع تولید، ارتقای بهره‌وری، کاهش هزینه‌های مبادلاتی، ایجاد اشتغال و کاهش تورم برخوردار بوده و در رشد درون‌زای اقتصادی نقش مهمی دارد.

بهره‌گیری از مزایای تکنولوژی اطلاعات در تجارت الکترونیکی مستلزم شناخت کاملی از ویژگیها و بسترهای حقوقی در قانون توسعه تجارت الکترونیک و بانکداری الکترونیکی است. یکی از این زیرساختهای مهم در مقبولیت برایندهای بانکداری الکترونیکی، امنیت و کنترل رفتارهای غیرقانونی در این نوع سیستمها است. منتهی به عنوان یکی از چالشهای توسعه تجارت و بانکداری الکترونیکی در جهت کاهش ریسک در بازار فعالان تجارت الکترونیک و بانکها مطرح بوده و از مهمترین پارامترهای تضمین سلامت تراکنش‌های مالی محسوب می‌شود. هر سیستم بانکداری الکترونیکی باید عوامل تصدیق اصالت، محرمانگی، انکارناپذیری و دیگر پارامترهای امنیتی را در نظر داشته و تضمین کند که فقط افراد مبادرت‌کنندگان به اطلاعات مجاز، محرمانه و حسابهای مشتریان دسترسی داشته و سوابق معاملات، غیرقابل ردیابی و رسیدگی باشند. مسئله اعتماد در محیط اینترنت و بانکداری الکترونیکی مهم‌تر از تجارت و فروش و بانکداری در محیط آفلاین است زیرا ایجاد و پرورش اعتماد وقتی مهم است که عدم اطمینان و ریسک فراگیر باشد.

بنابراین برای توسعه تجارت الکترونیکی به مجموعه اقدامات اساسی در زمینه‌های زیرساخت فنی، مسائل قانونی و مقرراتی، آگاه‌سازی و آموزش و تحصیل، فراهم آوری بسترهای امنیتی در زمینه تجارت الکترونیک و بانکداری اینترنتی است تا شرایط برای فعالیت فعالان اقتصادی یعنی مصرف‌کنندگان و بنگاه‌ها که نقش محوری در بکارگیری تجارت الکترونیکی دارند، فراهم شود.

واژه‌های کلیدی :

اینترنت، تجارت الکترونیک ، بانکداری الکترونیکی ، بانکداری اینترنتی ، پرداخت آنلاین ، امنیت ، قالب، رمزنگاری، احراز هویت، امضای دیجیتال، استانداردهای امنیتی.

فهرست مطالب

عنوان

شماره صفحه

فصل اول ، مقدمه

۱-۱- مقدمه مولفین.....	۲
۱-۲- مروری بر کتاب.....	۲
۱-۳- مسأله اصلی کتاب.....	۳
۱-۴- تشریح و بیان موضوع.....	۴
۱-۵- ضرورت انجام کتاب.....	۴
۱-۶- مدل تشریح کتاب (ارتباط متغیرها به صورت تصویری).....	۵
۱-۷- اهداف کتاب.....	۵
۱-۸- قلمرو انجام کتاب.....	۵
۱-۹- تعریف واژه‌ها و اصطلاحات تخصصی.....	۵
۱-۱۰- معماری کتاب.....	۸

۹	۲-۱- مقدمه
۹	۲-۲- تاریخچه تجارت الکترونیک و امنیت در پرداختهای آنلاین
۱۰	۲-۳- تعاریف تجارت الکترونیک و پرداخت آنلاین
۱۲	۲-۴- مدل های تجارت الکترونیکی
۱۳	۲-۴-۱- مدل Business to Business یا B۲B
۱۳	۲-۴-۲- مدل Business to Consumer یا B۲C و Consumer to Business یا C۲B
۱۳	۲-۴-۳- مدل Consumer to Consumer یا C۲C
۱۳	۲-۴-۴- مدل Government to Business یا G۲B و Business to Government یا B۲G
۱۳	۲-۴-۵- مدل Government to Customer یا G۲C و Customer to Government یا C۲G
۱۳	۲-۴-۶- مدل Government to Government یا G۲G
۱۴	۲-۵- مزایای استفاده از تجارت الکترونیکی
۱۴	۲-۵-۱- دسترسی مناسب اطلاعات و ارتباطی
۱۴	۲-۵-۲- حذف نسبی واسطه ها
۱۴	۲-۵-۳- افزایش قدرت خریداران و فروش بازارهای جدید برای تولیدکنندگان
۱۴	۲-۵-۴- سفارشی کردن محصولات و خدمات مشتریانی قوی
۱۵	۲-۵-۵- پیدایش مؤسسات اقتصادی و رقابت سراسری
۱۵	۲-۶- چارچوب نظری تجارت الکترونیک
۱۶	۲-۷- مراحل تجارت الکترونیک
۱۷	۲-۸- تفاوت مبادله الکترونیکی داده ها با تجارت الکترونیک
۱۸	۲-۹- ابزارهای تجارت الکترونیک
۱۸	۲-۱۰- پرداخت الکترونیکی
۱۹	۲-۱۰-۱- روشهای پرداخت الکترونیکی
۱۹	۲-۱۰-۲- استفاده از کارتهای الکترونیکی
۲۰	۲-۱۰-۳- پول الکترونیکی
۲۰	۲-۱۰-۴- روش پرداخت شخص به شخص
۲۰	۲-۱۰-۵- چک الکترونیکی
۲۰	۲-۱۰-۶- کارت های هوشمند
۲۰	۲-۱۰-۶-۱- از نظر نوع ارتباط کارت با کارت خوان
۲۰	۲-۱۰-۶-۲- از نظر نوع تراشه بکار رفته در کارت
۲۱	۲-۱۰-۶-۳- امنیت کارتهای الکترونیکی
۲۱	۲-۱۱- آشنایی با پول الکترونیک
۲۱	۲-۱۱-۱- ویژگیهای پول الکترونیک
۲۳	۲-۱۱-۲- مشکلات مطرح در روش پول الکترونیکی
۲۳	۲-۱۱-۳- برقراری خاصیت ناشناس ماندن استفاده کنندگان پول الکترونیکی
۲۴	۲-۱۱-۴- جلوگیری از پرداخت مجدد پول الکترونیکی

۲۵	۲-۱۱-۵- پیامدهای اقتصادی گسترش استفاده از پول الکترونیکی
۲۵	۲-۱۱-۶- افزایش کارایی مبادلات
۲۵	۲-۱۱-۷- واسطه‌های مالی و بانکها
۲۶	۲-۱۱-۸- بازارهای مالی
۲۶	۲-۱۱-۹- رشد و توسعه کاربرد پول الکترونیک و مؤسسات پرداخت الکترونیک در جهان
۲۷	۲-۱۲- معماری اینترنت
۲۷	۲-۱۳- معماری WAP
۲۸	۲-۱۴- نتیجه‌گیری
	فصل سوم، امنیت و چالشهای امنیتی در تجارت الکترونیک و پرداخت‌های آنلاین
۳۰	۳-۱- مقدمه
۳۰	۳-۲- تعریف امنیت
۳۱	۳-۳- رویکردهای امنیتی
۳۲	۳-۱-۱- فرآیند امن‌سازی
۳۳	۳-۳-۲- پراخه حفاظت اطلاعات
۳۴	۳-۴- مفهوم امنیت در تجارت الکترونیک
۳۵	۳-۴-۱- امنیت در تولید
۳۶	۳-۴-۱-۱- Cross site scripting
۳۶	۳-۴-۱-۲- SQL Injection
۳۶	۳-۴-۱-۳- Price manipulation
۳۶	۳-۴-۱-۴- Buffer overflow
۳۷	۳-۴-۱-۵- Password guessing
۳۷	۳-۴-۲- امنیت در ارائه
۳۸	۳-۴-۳- امنیت در انتقال
۳۸	۳-۴-۴- امنیت در دریافت
۳۸	۳-۴-۵- مهندسی اجتماعی
۳۹	۳-۵- راهکارهای مقابله
۳۹	۳-۵-۱- تولید
۴۰	۳-۵-۲- ارائه
۴۱	۳-۵-۳- انتقال
۴۱	۳-۵-۴- دریافت
۴۱	۳-۶- راهکارهای کلان
۴۲	۳-۶-۱- انواع حملات بر حسب نحوه عملکرد
۴۲	۳-۶-۲- انواع حملات از نظر تاثیر در ارتباط
۴۳	۳-۷- تهدیدات امنیتی فضای مجازی
۴۳	۳-۷-۱- Phishing
۴۴	۳-۷-۲- Pharming

۴۴	۳-۷-۳- ویروس ها و کرم ها
۴۵	۳-۷-۴- تروژان ها
۴۵	۳-۷-۵- DOS
۴۶	۳-۸- روشهای برقراری امنیت در قراردادهای الکترونیکی
۴۶	۳-۸-۱- تهدیدها
۴۷	۳-۸-۲- اهداف
۴۸	۳-۸-۳- محرمانه بودن پیام
۴۸	۳-۸-۴- شناسایی متعاملین و کنترل دسترسی
۴۹	۳-۸-۵- تأیید اصالت
۵۰	۳-۸-۵- عدم رد
۵۰	۳-۸-۶- تمام داده
۵۱	۳-۹- نیازمندیهای امنیت
۵۲	۳-۱۰- هزینه در ازای امنیت
۵۳	۳-۱۱- امنیت مخابرات در کاربر یک
۵۳	۳-۱۱-۱- SSL/TLS/WTLS
۵۳	۳-۱۱-۲- کانال ایمن
۵۳	۳-۱۱-۳- توافق و انتقال داده
۵۳	۳-۱۱-۴- TLS/SSLV/SSLV
۵۴	۳-۱۱-۵- WTLS
۵۴	۳-۱۱-۶- مسایل پیاده سازی
۵۴	۳-۱۱-۷- تکیه گاههای اعتماد
۵۵	۳-۱۱-۸- محدودیت های صادراتی
۵۵	۳-۱۲- اعتبارسنجی کاربر
۵۵	۳-۱۲-۱- موجودیت در برابر اعتبارسنجی تراکش
۵۵	۳-۱۲-۲- مکانیزم تصدیق
۵۵	۳-۱۲-۲-۱- رمز با طول ثابت
۵۶	۳-۱۲-۲-۲- رمز پویا
۵۶	۳-۱۲-۲-۳- پرسش / پاسخ
۵۷	۳-۱۲-۲-۴- SSL/TLS/WTLS
۵۷	۳-۱۲-۲-۵- امنای دیجیتال
۵۷	۳-۱۲-۲-۶- مجوزهای سخت افزاری
۵۸	۳-۱۳- مطالب بیشتر راجع به امنیت
۵۸	۳-۱۳-۱- ثبت نام
۵۸	۳-۱۳-۲- وکالت و نمایندگی
۵۸	۳-۱۳-۳- بسترهای امن
۵۹	۳-۱۳-۴- عامل انسانی

۵۹	۵-۱۳-۳- ورود به کامپیوتر و کنترل عملیات
۵۹	۱۴-۳- نتیجه گیری
	فصل چهارم ، رمز نگاری
۶۲	۱-۴- مقدمه
۶۲	۲-۴- تعریف رمزنگاری
۶۳	۳-۴- دلیل رمزنگاری اطلاعات در کامپیوتر
۶۳	۴-۴- دو اصل اساسی رمز نگاری
۶۴	۵-۴- سرویس رمزنگاری
۶۵	۶-۴- رمزنگاری سخت افزاری
۶۵	۷-۴- پروتکل رمزنگاری
۶۶	۸-۴- الگوریتم رمزنگاری
۶۷	۹-۴- انواع روش های رمزنگاری
۶۷	۱-۹-۴- رمزهای جانشینی
۶۸	۲-۹-۴- رمزهای جابجایی
۶۸	۱۱-۴- الگوریتمهای رمزنگاری متقارن
۷۰	۱-۱۱-۴- روش متقارن رمزنگاری
۷۱	۲-۱۱-۴- تحلیل الگوریتمهای نامتقارن
۷۱	۱۲-۴- الگوریتمهای رمزنگاری نامتقارن
۷۶	۱-۱۲-۴- تحلیل الگوریتمهای نامتقارن
۷۶	۱۳-۴- رمزنگاری کلید عمومی
۷۶	۱۴-۴- الگوریتمهای رمزنگاری کلید خصوصی
۷۷	۱۵-۴- تکنولوژی امنیتی PKI
۷۹	۱۶-۴- مقایسه روشهای رمزنگاری
۸۰	۱۷-۴- انواع کلیدهای رمزنگاری
۸۰	۱-۱۷-۴- کلیدهای محرمانه
۸۱	۲-۱۷-۴- کلیدهای عمومی و خصوصی
۸۲	۳-۱۷-۴- کلیدهای اصلی و کلیدهای مشتق شده
۸۲	۴-۱۷-۴- کلیدهای رمز کننده کلید
۸۳	۵-۱۷-۴- کلیدهای نشست
۸۳	۱۸-۴- رمزنگاری مبدأ به مقصد و رمزنگاری انتقال
۸۴	۱۹-۴- تجزیه و تحلیل رمز
۸۵	۱-۱۹-۴- افرونگی
۸۵	۲-۱۹-۴- تازگی پیامها
۸۵	۳-۱۹-۴- راهکاری برای ایجاد تازگی پیام
۸۵	۴-۱۹-۴- رمزهای دنباله ای
۸۵	۲۰-۴- مدیریت کلید

۸۶	۴-۲۰-۱- دریافت و استفاده از زوج کلید
۸۶	۴-۲۰-۲- بازیابی کلید
۸۶	۴-۲۰-۳- چرخه حیات یک کلید
۸۷	۴-۲۱- رمز نگاری Rijndael
۸۹	۴-۲۲- الگوریتم آمیزش
۹۰	۴-۲۳- TLS و SSL
۹۰	۴-۲۴- الگوریتم های تبادل کلید
۹۱	۴-۲۵- نتیجه گیری
	فصل پنجم ، تشخیص هویت و امضای دیجیتالی
۹۳	۵-۱- مقدمه
۹۳	۵-۲- شناسایی احراز هویت
۹۴	۵-۲-۱- انواع دستورهای احراز هویت در امنیت اطلاعات
۹۴	۵-۲-۲- چیزی که شما می دانید
۹۵	۵-۲-۳- چیزی که ما داریم
۹۵	۵-۲-۴- چیزی که ما شنیدیم
۹۵	۵-۲-۵- منظور از Multi-Factor و Multi-step در احراز هویت
۹۶	۵-۳- رمز های عبور و توکن و بایومتریک
۹۷	۵-۳-۱- رمزهای عبور
۹۸	۵-۳-۲- توکن ها
۹۹	۵-۳-۳- سیستم های بایومتریک
۱۰۰	۵-۳-۳-۱- مقیاس های کارایی تجهیزات بایومتریک
۱۰۲	۵-۴- تعریف و تاریخچه امضای الکترونیک
۱۰۲	۵-۴-۱- تعریف امضاء و جایگاه حقوقی آن
۱۰۳	۵-۴-۲- تاریخچه امضای الکترونیک
۱۰۳	۵-۴-۳- تعریف امضای الکترونیک
۱۰۵	۵-۵- جنبه های فنی امضای الکترونیک
۱۰۵	۵-۵-۱- انواع امضای الکترونیک
۱۰۶	۵-۵-۲- فن آوری و زیرساخت امضای دیجیتال
۱۰۷	۵-۵-۳- امضای دیجیتالی مبتنی بر چکیده پیام
۱۰۸	۵-۵-۴- امضای دیجیتالی مبتنی بر روش های رمزنگاری کلید عمومی
۱۰۸	۵-۵-۵- مقایسه کلی امضای دیجیتال و گواهی نامه دیجیتال
۱۱۱	۵-۵-۶- معرفی الگوریتم درهم سازی استاندارد SHA-۲
۱۱۴	۵-۱۰- نحوه ایجاد یک امضای دیجیتال
۱۱۴	۵-۱۰-۱- مرجع گواهی امضاء
۱۱۶	۵-۱۰-۲- جنبه های حقوقی امضای الکترونیک
۱۱۷	۵-۱۰-۳- ماهیت امضای الکترونیکی

۱۱۷	۵-۱۰-۴- پذیرش قانونی امضای الکترونیک
۱۱۸	۵-۱۰-۵- ارزش اثباتی امضای الکترونیک
۱۱۸	۵-۱۱-۵- پسوردهای یکبار مصرف (OTP)
۱۱۹	۵-۱۱-۱- استفاده از شناسه کاربری و پسورد برای ورود به سیستم از طریق ریموت
۱۱۹	۵-۱۱-۲- استفاده از OTP برای وارد شدن به ویندوز از طریق ریموت
۱۲۰	۵-۱۱-۳- استفاده از OTP در کنار شبکه شرکت برای وارد شدن به سیستم عامل
۱۲۰	۵-۱۱-۴- استفاده از OTP برای دسترسی آفلاین
۱۲۰	۵-۱۱-۵- معماری پیشرفته
۱۲۱	۵-۱۱-۶- مزایای استفاده از این روش
۱۲۱	۵-۱۱-۷- مولفه‌ها و پیش‌نیازهای مورد احتیاج
۱۲۲	۵-۱۲- نحوه گیری
	فصل ششم، رکن هاوالگوریتم های امنیتی در تجارت الکترونیک و پرداختهای آنلاین
۱۲۴	۶-۱- مقدمه
۱۲۴	۶-۲- پروتکل PKI
۱۲۵	۶-۳- پروتکل SET
۱۲۶	۶-۳-۱- مدل SET
۱۲۷	۶-۳-۲- بررسی اجمالی از مدل SET
۱۲۷	۶-۳-۲-۱- مشکل با SSL
۱۲۷	۶-۳-۲-۲- بازنگری پروتکل SET
۱۲۹	۶-۳-۳-۱- استفاده از کلید متقارن
۱۲۹	۶-۳-۳-۲- استفاده از کلید نامتقارن- امضاء دیجیتال (خلاصه پیام)
۱۳۰	۶-۳-۳-۳- RSA-OAEP
۱۳۰	۶-۳-۴- امضاهای دوگانه
۱۳۰	۶-۳-۵- فرایند SET
۱۳۱	۶-۳-۶- بیمه گواهینامه
۱۳۲	۶-۳-۶-۱- گواهی نامه‌های تجاری
۱۳۲	۶-۳-۶-۲- گواهینامه دروازه پرداخت
۱۳۲	۶-۳-۶-۳- گواهینامه صادر کننده
۱۳۲	۶-۳-۷- ثبت نام شرکت کنندگان
۱۳۳	۶-۳-۸- دو مشکل با پروتکل ثبت نام
۱۳۳	۶-۳-۹- آینده SET
۱۳۴	۶-۴- پروتکل S-HTTP
۱۳۴	۶-۵- پروتکل S-MIME
۱۳۵	۶-۶- پروتکل SSL
۱۳۵	۶-۶-۱- مکانیزم های تشکیل دهنده SSL
۱۳۶	۶-۶-۲- اجزای پروتکل SSL

۱۳۶	۳-۶-۶- الگوریتم های رمزنگاری پشتیبانی شده در SSL
۱۳۶	۴-۶-۶- نحوه عملکرد داخلی پروتکل SSL
۱۳۷	۵-۶-۶- الگوریتم های رمزنگاری پشتیبانی شده در SSL
۱۳۸	۶-۶-۶- پروتکل رکورد در SSL
۱۳۸	۷-۶-۶- پروتکل تغییر مشخصات رمز در SSL
۱۳۸	۸-۶-۶- پروتکل هشدار در SSL
۱۳۸	۹-۶-۶- پروتکل دست دادن در SSL
۱۳۹	۷-۶- پروتکل SEPP
۱۳۹	۸-۶- پروتکل PCT
۱۴۰	۹-۶- پروتکل IPSec
۱۴۰	۱-۹-۶- حالت های انتقال و تونل در AH
۱۴۲	۲-۹-۶- پروتکل A
۱۴۳	۳-۹-۶- پروتکل ESP
۱۴۴	۴-۹-۶- پروتکل IKE
۱۴۵	۱۰-۶- معرفی پروتکل Authn
۱۴۶	۱-۱۰-۶- نقاط ضعفberos
۱۴۶	۱۱-۶- پروتکل SESAME
۱۴۷	۱۲-۶- پروتکل Kryptonite
۱۴۷	۱۳-۶- پروتکل های انتقال فایل امن
۱۴۷	۱-۱۳-۶- ASZ
۱۴۸	۲-۱۳-۶- FTP
۱۴۸	۳-۱۳-۶- FTPS و SFTP
۱۴۹	۱۴-۶- پروتکل امنیتی TLS
۱۵۰	۱۵-۶- امنیت لایه انتقال
۱۵۱	۱۶-۶- پروتکل تبادل کلید دیفی ، هلمن
۱۵۲	۱۷-۶- توابع درهم ساز
۱۵۲	۱-۱۷-۶- اس اچ ای-۱
۱۵۳	۲-۱۷-۶- مقایسه ای میان توابع درهم سازی
۱۵۳	۳-۱۷-۶- کاربردها
۱۵۴	۴-۱۷-۶- صحت داده
۱۵۴	۵-۱۷-۶- آنالیز و ارزیابی رمزنگاری
۱۵۴	۶-۱۷-۶- SHA-۰۰
۱۵۵	۷-۱۷-۶- اس اچ ای-۲
۱۵۶	۱۸-۶- استاندارد X.۵۰۹
۱۵۶	۱-۱۸-۶- ساختار گواهی
۱۵۷	۲-۱۸-۶- فیلد Extension