مفاهیم و ویژگی‌های

امضای دیجیتال

دکتر علی عبدالهی
مهندس طاهره منزوی
مهندس یونس جهان جری

سرشناسه: عبداللهی، علی، ۱۳۵۵-
عنوان و نام پدیدآور : مفاهیم و ویژگی‌های امضای دیجیتال/ علی عبداللهی، طاهره منزوی، یونس جوان‌چری.
مشخصات نشر : تهران: سازمان بورس اوراق بهادار، شرکت اطلاع رسانی و خدمات بورس تهران، ۱۳۸۹.
مشخصات ظاهری : ۱۱۲ ص.: مصور، جدول.
شابک : ۲۵۰۰۰ ریال: ۲-۰۶-۵۹۵۹-۶۰۰-۹۷۸
وضعیت فهرست نویسی : فیپا
موضوع : امضای الکترونیکی -- قوانین و مقررات
موضوع : امضای الکترونیکی
شناسه افزوده : منزوی، طاهره، ۱۳۵۲ -
شناسه افزوده : جوان‌چری، یونس، ۱۳۵۷ -
شناسه افزوده : شرکت اطلاع رسانی و خدمات بورس تهران
رده بندی کنگره : ۱۳۸۹ ۲ع۲ک/ K۵۶۴
رده بندی دیویی : ۳۴۳/۰۹۹۴۴
شماره کتابشناسی ملی: ۲۱۳۷۰۹۱

مفاهیم و ویژگی‌های امضای دیجیتال

مؤلفان: دکتر علی عبداللهی، مهندس طاهره منزوی، مهندس یونس جوان‌چری
ناشر: شرکت اطلاع‌رسانی و خدمات بورس
مدیر هنری: رسول خسروبیگی
چاپ و صحافی: خجسته
چاپ اول: ۱۳۸۹
قیمت: ۲۵۰۰۰ ریال
شمارگان: ۲۵۰۰ نسخه
شابک: ۲-۰۶-۵۹۵۹-۶۰۰-۹۷۸

فهرست مطالب

فصل چهارم: زیرساخت کلید عمومی و رویکردهای پیاده سازی آن

فصل پنجم: قوانین امضای دیجیتال

فصل ششم: موردکاویها

منابع و مراجع

پیشگفتار

استفاده از فناوری امضای دیجیتال در سال های اخیر رشد زیادی داشته، بطوریکه بسیاری بر این باورند انجام تجارت و تبادلات الکترونیکی بدون بکارگیری امضای دیجیتال از امنیت و قابلیت اعتماد لازم برخوردار نیست. از آن جا که اطلاعات مهم‌ترین دارایی بازار سرمایه است، بکارگیری امضای دیجیتال در بازار سرمایه نیز از اهمیت بالایی برخوردار است. تبادل مدارک، مستندات و اطلاعات بین ارکان و فعالان بازار سرمایه و همچنین انجام معاملات برخط در بورس ها و بازارهای خارج از بورس بدون بکارگیری امضای دیجیتال ریسک های زیادی به همراه دارد.

امضای دیجیتال ابزاری توانمند برای تأمین امنیت ارتباط بین بخش های مختلف بازار سرمایه از قبیل شرکت‌های پذیرفته شده در بورس، کارگزاران، نهادهای مالی، سهامداران و ... محسوب می شود. در همین راستا، سازمان بورس و اوراق بهادار با هدف شناسایی و احراز هویت ارسال کنندگان اطلاعات، اطمینان از دسترسی افراد مجاز به اطلاعات، جلوگیری از افشای غیرمجاز اطلاعات، اطمینان از عدم تغییر و دستکاری اطلاعات، افزایش قابلیت اعتمادپذیری آن، و در نهایت تسهیل ارتباطات الکترونیکی در بازار سرمایه اقدام به بکارگیری امضای دیجیتال در سامانه های نرم افزاری خود مانند سامانه تبادل اطلاعات نهاد های مالی(ستان) و سامانه یکپارچهٔ گردآوری و انتشار الکترونیکی اطلاعات ناشران(کدال) نموده است.

با توجه به نقش مهم و کلیدی فناوری اطلاعات در توسعه بازار سرمایه، فرهنگ سازی و درک مفاهیم مرتبط با این فناوری مقدمه ای برای بکارگیری مؤثرتر آن بوده و موجبات افزایش کارایی بازار سرمایه را فراهم می آورد. کتاب حاضر با هدف آشنایی هر چه بیشتر فعالان بازار سرمایه و دیگر علاقمندان با فناوری امضای دیجیتال و مفاهیم آن تهیه و تنظیم شده است. امید است خوانندگان بتوانند با بهره گیری لازم از مطالب این کتاب، زمینه را برای توسعه و بکارگیری هر چه بهتر این فناوری در بازار سرمایه و همچنین دیگر حوزه های مرتبط فراهم آورند.

دکتر علی صالح آبادی
رئیس سازمان بورس و اوراق بهادار

مقدمه

دو هزار سال پیش پاپیروس تنها راه ارتباط مکتوب افراد با یکدیگر بود. تا چندی پیش نیز مدارک و سوابق بر روی کاغذ تهیه شده و تأیید آنها توسط امضای دستی صورت می‌گرفت. امروزه تحول فناوری باعث ناکارآمدی روشهای کاغذی شده و بیشتر ارتباطات کسب و کاری از شکل کاغذی به شکل الکترونیکی تغییر یافته است. در دنیای دیجیتال امروز، حجم مستندات الکترونیکی ایجاد شده از روندی رو به رشد برخوردار است. در سیستمهای پیشرفته، داده‌ها به صورت الکترونیکی ایجاد، ویرایش و پردازش شده و در نهایت نیز به صورت الکترونیکی بایگانی می‌شوند. تبادلات تجاری به حجم روزانه میلیاردها دلار، با استفاده از اینترنت انجام می‌گیرد. بسیاری از موسسات مالی نیز برای انتقال داده‌ها از بستر اینترنت استفاده می‌کنند. مزایای استفاده از مستندات الکترونیکی بر کسی پوشیده نیست. کیفیت و هزینه مطلوب این نوع اطلاعات مزایای بیشماری در تمامی بخشهای اقتصاد و جامعه دارد. اما از طرفی، مستندات و اطلاعات الکترونیکی در معرض سوءاستفاده و آسیبهای فراوانی نیز هستند.

در جعل اطلاعات الکترونیکی هیچ اثری از مجرم باقی نمی‌ماند و مستندات

الکترونیکی را می‌توان به راحتی کپی و دستکاری نمود، لذا نباید همیشه آنها را صحیح و قابل اعتماد فرض کرد. علاوه بر این، حین انتقال اطلاعات از طریق اینترنت امکان دسترسی غیرمجاز و افشای اطلاعات حساس وجود دارد. بنابراین امنیت مستندات الکترونیکی باید به گونه‌ای تأمین گردد که گیرنده بتواند به درستی محتوای مستندات(جامعیت) اعتماد کرده و فرستنده نیز نتواند بعدها آن را انکار نماید(انکارناپذیری). همزمان با شتاب گرفتن روند تبدیل مستندات کاغذی به الکترونیکی، بحث پیامدهای قانونی ایجاد، دریافت و انتقال این مستندات مستلزم توجهی شایسته است.

در این کتاب سعی شده مفاهیم رمزنگاری و امضای دیجیتال به زبانی ساده و قابل فهم بیان شود.

در فصل اول، امنیت در دنیای مجازی با امنیت در دنیای واقعی مقایسه شده و از این طریق روشهای احراز هویت در اینترنت و الزامات امنیتی معمول در این فضا تشریح شده است.

فصل دوم مروری کوتاه بر تاریخچه امضای دیجیتال، مزایای آن، مکانیزم امضای دیجیتال، الگوریتم‌های امضای دیجیتال، رمزنگاری و انواع روشهای آن و دیگر مباحث مرتبط خواهد داشت.

فصل سوم شامل مباحث مرتبط با گواهینامه دیجیتال، مراکز صدور این گواهینامه‌ها(CAها)، مدیریت گواهینامه‌های دیجیتال، گواهینامه بین مراجع، سطوح مختلف گواهینامه و کاربرد گواهینامه دیجیتال در تبادلات اینترنتی(پروتکل‌های SET ، SSL و S/MIME)... است.

فصل چهارم به زیرساخت کلید عمومی و اجزای اصلی آن، سیاستها، رویه‌ها و اقدامات CAها، عملیاتی نمودن یک CA، مدلهای مختلف ایجاد CA و مباحث مختلف فنی، کسب و کاری و قانونی مربوط به پیاده سازی CA می‌پردازد.

فصل پنجم مروری بر تاریخچه توسعه قوانین امضای دیجیتال و قوانین آن در کشورهای مختلف دارد.

در فصل ششم نیز چند موردکاوی در این زمینه بررسی شده است.