ÖZET

BİR XML İMZA OLUŞTURMA SİSTEMİ VE YÖNTEMİ

Bu buluş, e-fatura, e-belge gibi dijital dökümanlar için elektronik imza kullanan tüm ortamlarda kullanılan ve XML (Extensible Markup Language - Genişletilebilir İşaretleme Dili) imzalı dosyaların (A) oluşturulmasını sağlayan bir sistem (1) ve yöntem (1000) ile ilgilidir. Sistem (1), XML dosyalarının (A) ve sertifika dosyalarının (B) saklandığı yer olan depolama birimi (2) ve hafıza ve işlemciye sahip olan be imzalama işlemini gerçekleştiren kontrol birimi (3) içermektedir.

İSTEMLER

1. XML dosyalarının (A) ve sertifika dosyalarının (B) saklandığı yer olan depolama birimi (2) sahip olan, e-fatura, e-belge gibi dijital dökümanlar için elektronik imza kullanan tüm ortamlarda kullanılan ve XML (Extensible Markup Language - Genişletilebilir İşaretleme Dili) imzalı dosyaların (A) oluşturulmasını sağlayan bir sistem (1) olup, **özelliği;**

- ❖ hafıza ve işlemciye sahip olan, imzalama işlemini gerçekleştiren ve
  - o depolama biriminden (2) sertifika dosyasının (B) okunması,
  - o sertifika dosyasının (B) içerisinden işlevsiz (dummy) bir test datası ile sertifika anlamsız verilerinin (hash) elde edilmesi, bu verilerin içeriklerinin silinip uzunluklarının sabit bırakılması, bu şekilde uzunlukları sabit fakat hash datası boş karakterden oluşan binary formatın elde edilmesi ve hash datalarının başlangıç ve bitiş adreslerinin hafızada saklanması,
  - o depolama biriminden (2) XML dosyasının (A) binary olarak okunması ve XML dosyasının (A) içerisindeki datanın başlangıç adresinin tespit edilirek hafızada saklanması,
  - o XML dosyasının (A) içerisinde bulunan XML datasının (innerXML), bulunduğu başlangıç adresinden itibaren binary olarak elde edilmesi,
  - o elde edilen binary datadan seritifika hash datalarının manuel hesaplanması (digest hash, signature hash gibi),
  - o daha önce oluşturulan boş sertifika formatının kopyalanması, boş alanlara hesaplanan hash değerleri yazılarak binary yapının elde edilmesi ve bu yazma işlemlerinin binary olarak yapılması,
  - o sertifika binary datası ile gerçek XML datanın uç uca binary olarak birleştirilerek yeni binary yapının oluşturulması ve
  - o birleştirilen bu binary yapının XML uzantılı dosya (A) olarak depolama birimine (2) yazılması

işlemlerini gerçekleştirmek için konfigüre edilmiş olan kontrol birimi (3) içermesidir.

2. E-fatura, e-belge gibi dijital dökümanlar için elektronik imza kullanan tüm ortamlarda kullanılan ve XML (Extensible Markup Language - Genişletilebilir İşaretleme Dili) imzalı dosyaların (A) oluşturulmasını sağlayan yöntem (1000) olup, **özelliği;**

- ❖ kontrol birimi (3) vasıtasıyla, depolama biriminden (2) sertifika dosyasının (B) okunması (1001),
- ❖ kontrol birimi (3) vasıtasıyla, sertifika dosyasının (B) içerisinden işlevsiz (dummy) bir test datası ile sertifika anlamsız verilerinin (hash) elde edilmesi, bu verilerin içeriklerinin silinip uzunluklarının sabit bırakılması, bu şekilde uzunlukları sabit fakat hash datası boş karakterden oluşan binary formatın elde edilmesi ve hash datalarının başlangıç ve bitiş adreslerinin hafızada saklanması (1002),
- ❖ kontrol birimi (3) vasıtasıyla, depolama biriminden (2) XML dosyasının (A) binary olarak okunması ve XML dosyasının (A) içerisindeki datanın başlangıç adresinin tespit edilirek hafızada saklanması (1003),
- ❖ kontrol birimi (3) vasıtasıyla, XML dosyasının (A) içerisinde bulunan XML datasının (innerXML), bulunduğu başlangıç adresinden itibaren binary olarak elde edilmesi (1004),
- ❖ kontrol birimi (3) vasıtasıyla, elde edilen binary datadan seritifika hash datalarının manuel hesaplanması (digest hash, signature hash gibi) (1005),
- ❖ kontrol birimi (3) vasıtasıyla, daha önce oluşturulan boş sertifika formatının kopyalanması, boş alanlara hesaplanan hash değerleri yazılarak binary yapının elde edilmesi ve bu yazma işlemlerinin binary olarak yapılması (1006),
- ❖ kontrol birimi (3) vasıtasıyla, sertifika binary datası ile gerçek XML datanın uç uca binary olarak birleştirilerek yeni binary yapının oluşturulması (1007) ve

- kontrol birimi (3) vasıtasıyla, birleştirilen bu binary yapının XML uzantılı dosya (A) olarak depolama birimine (2) yazılması (1008)

işlem adımlarını içermesidir.

TARİFNAME

BİR XML İMZA OLUŞTURMA SİSTEMİ VE YÖNTEMİ

Teknik Alan

Bu buluş, e-fatura, e-belge gibi dijital dökümanlar için elektronik imza kullanan tüm ortamlarda kullanılan ve XML (Extensible Markup Language - Genişletilebilir İşaretleme Dili) imzalı dosyaların (A) oluşturulmasını sağlayan bir sistem ve yöntem ile ilgilidir.

Tekniğin Bilinen Durumu

Mevcut yöntemde uygulama vasıtasıyla XML döküman sisteme yüklenir. Tüm veriler okunarak algoritma ile anlamsız veri (hash) değeri üretilir. Daha sonra oluşan hash değeri dokümana eklenerek yeni bir XML oluşturulur.

Bu yöntem ile XML dosyası okunarak tamamı sisteme XML formatından çevrilmekte ve XML objesi oluşturulmaktadır. Hash değeri hesaplandıktan sonra bu değer ayrı XML etiketi (tag) olarak XML objesinin başına eklenmektedir. Bunun için diğer XML objelerinin aşağı kaydırılması gerekmektedir. Daha sonrasında yeni XML objesi dosyaya yazılmaktadır. Bu işlem her bir dosya için tek tek yapılmaktadır. Milyonlarca adet dosya olduğu düşünüldüğünde, söz konusu işlem uzun süreler almaktadır.

Tekniğin bilinen durumunda yer alan TR2020/13877 numaralı patent başvuru dokümanında, XML dosyalarında otomatik etiket kontrol sistemi açıklanmaktadır. İlgili dokümanda yer alan sistemde, e-fatura, e-belge gibi dijital dökümanlar için elektronik imza kullanan tüm ortamlarda kullanılan ve XML (Extensible Markup Language - Genişletilebilir İşaretleme Dili) imzalı dosyaların (A) oluşturulmasını sağlayan bir yapılanma bulunmamaktadır.

Sonuç olarak, yukarıda anlatılan ihtiyaçları karşılayacak çözümlerin konu hakkındaki yetersizliği nedeniyle ilgili teknik alanda bir geliştirme yapılması gerekli kılınmıştır.

Buluşun Amacı

Buluş, mevcut durumlardan esinlenerek oluşturulup yukarıda belirtilen olumsuzlukları çözmeyi amaçlamaktadır.

Bu buluşun amacı e-fatura, e-belge gibi dijital dökümanlar için elektronik imza kullanan tüm ortamlarda kullanılan ve XML (Extensible Markup Language - Genişletilebilir İşaretleme Dili) imzalı dosyaların (A) oluşturulmasını sağlayan bir sistem ve yöntemin ortaya konulmasıdır.

Buluşun yapısal ve karakteristik özellikleri ve tüm avantajları aşağıda verilen şekiller ve bu şekillere atıflar yapılmak suretiyle yazılan detaylı açıklama sayesinde daha net olarak anlaşılacaktır ve bu nedenle değerlendirmenin de bu şekiller ve detaylı açıklama göz önüne alınarak yapılması gerekmektedir.

Buluşun Anlaşılmasına Yardımcı Olacak Şekiller

Şekil 1, buluşa konu olan sistemin şematik gösterimidir.

Şekil 2, buluşa konu olan yönteme ait akış diyagramıdır.

Parça Referanslarının Açıklaması

1. Sistem
2. Depolama birimi
3. Kontrol birimi

1000. Yöntem

A. XML dosyası

B. Sertifika dosyası

Buluşun Detaylı Açıklaması

Bu detaylı açıklamada, buluşa konu olan sistem (1) ve yöntemin (1000) tercih edilen yapılanmaları, sadece konunun daha iyi anlaşılmasına yönelik olarak açıklanmaktadır.

Bu buluş, e-fatura, e-belge gibi dijital dökümanlar için elektronik imza kullanan tüm ortamlarda kullanılan ve XML (Extensible Markup Language - Genişletilebilir İşaretleme Dili) imzalı dosyaların (A) oluşturulmasını sağlayan bir sistem (1) ve yöntem (1000) ile ilgilidir.

Şekil1'de şematik gösterimi sunulan buluş konusu sistem (1);

- XML dosyalarının (A) ve sertifika dosyalarının (B) saklandığı yer olan depolama birimi (2) ve
- hafıza ve işlemciye sahip olan, imzalama işlemini gerçekleştiren ve
  - depolama biriminden (2) sertifika dosyasının (B) okunması,
  - sertifika dosyasının (B) içerisinden işlevsiz (dummy) bir test datası ile sertifika anlamsız verilerinin (hash) elde edilmesi, bu verilerin içeriklerinin silinip uzunluklarının sabit bırakılması, bu şekilde uzunlukları sabit fakat hash datası boş karakterden oluşan binary formatın elde edilmesi ve hash datalarının başlangıç ve bitiş adreslerinin hafızada saklanması,
  - depolama biriminden (2) XML dosyasının (A) binary olarak okunması ve XML dosyasının (A) içerisindeki datanın başlangıç adresinin tespit edilirek hafızada saklanması,
  - XML dosyasının (A) içerisinde bulunan XML datasının (innerXML), bulunduğu başlangıç adresinden itibaren binary olarak elde edilmesi,
  - elde edilen binary datadan seritifika hash datalarının manuel hesaplanması (digest hash, signature hash gibi),
  - daha önce oluşturulan boş sertifika formatının kopyalanması, boş alanlara hesaplanan hash değerleri yazılarak binary yapının elde edilmesi ve bu yazma işlemlerinin binary olarak yapılması,
  - sertifika binary datası ile gerçek XML datanın uç uca binary olarak birleştirilerek yeni binary yapının oluşturulması ve
  - birleştirilen bu binary yapının XML uzantılı dosya (A) olarak depolama birimine (2) yazılması

  işlemlerini gerçekleştirmek için konfigüre edilmiş olan kontrol birimi (3)

içermektedir.

Sistem (1), günümüzde kullanılan yapılardaki performans sorunun ortadan kaldırmak için bir yöntem (1000) kullanmaktadır. 1 milyon adet XML dosyasının (A) üretildiği

düşünülsün. Bu üretilen dosyaların (A) başlangıç değerleri aynıdır. Dosya (A) binary olarak açıldığında, her bir dosyanın (A) datası belirli bir kaydırmadan (offset) başlar. Örneğin 224. byte'tan itibaren datalar dosyanın (A) içeriğine göre değişir. Fakat 0-224 byte arası değerler aynıdır. Sistem (1) bu başlangıç offset'ini bildiği için, 225. byte'tan itibaren dosyayı (A) binary olarak okumakta, dataya erişmekte ve buradan işaret değeri (sign value) üretmektedir. Sistem (1), bu üretilen binary data ile gerçek XML binary datayı uç uca birleştirerek dosyaya (A) yazmaktadır. Bu durumda XML'le objeye çevirmeye ve hesaplanan işaret değerini araya eklemeye gerek kalmadan hız bir şekilde dosya (A) elde edilmektedir.

Şekil2'de akış diyagramı sunulan buluş konusu yöntem (1000);

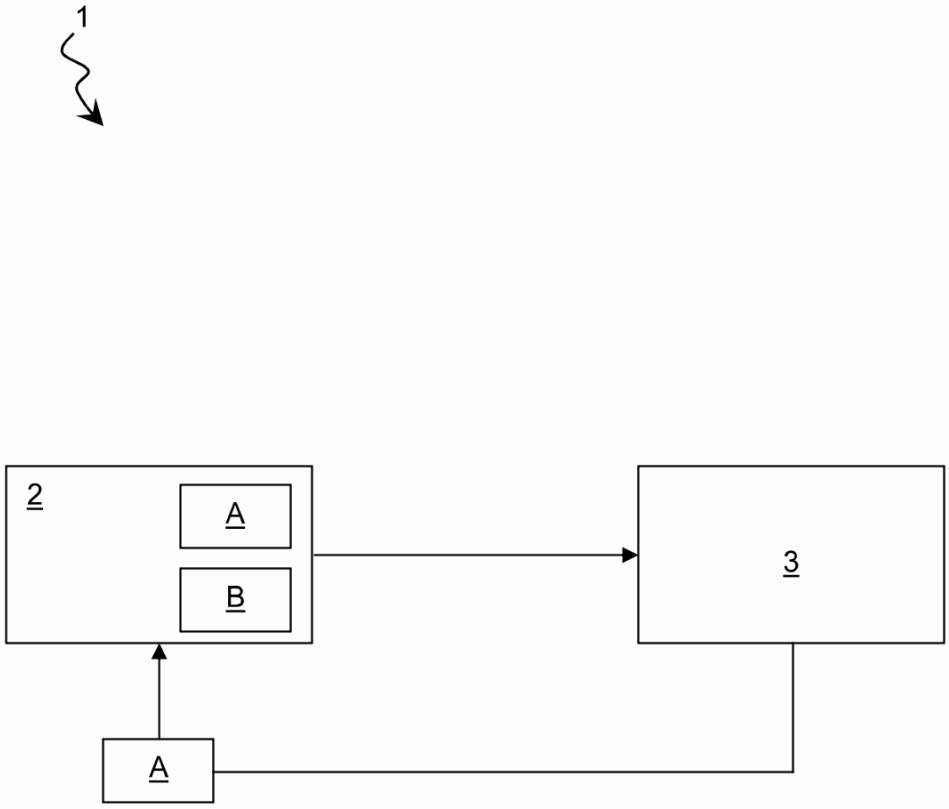
- kontrol birimi (3) vasıtasıyla, depolama biriminden (2) sertifika dosyasının (B) okunması (1001),
- kontrol birimi (3) vasıtasıyla, sertifika dosyasının (B) içerisinden işlevsiz (dummy) bir test datası ile sertifika anlamsız verilerinin (hash) elde edilmesi, bu verilerin içeriklerinin silinip uzunluklarının sabit bırakılması, bu şekilde uzunlukları sabit fakat hash datası boş karakterden oluşan binary formatın elde edilmesi ve hash datalarının başlangıç ve bitiş adreslerinin hafızada saklanması (1002),
- kontrol birimi (3) vasıtasıyla, depolama biriminden (2) XML dosyasının (A) binary olarak okunması ve XML dosyasının (A) içerisindeki datanın başlangıç adresinin tespit edilirek hafızada saklanması (1003),
- kontrol birimi (3) vasıtasıyla, XML dosyasının (A) içerisinde bulunan XML datasının (innerXML), bulunduğu başlangıç adresinden itibaren binary olarak elde edilmesi (1004),
- kontrol birimi (3) vasıtasıyla, elde edilen binary datadan seritifika hash datalarının manuel hesaplanması (digest hash, signature hash gibi) (1005),
- kontrol birimi (3) vasıtasıyla, daha önce oluşturulan boş sertifika formatının kopyalanması, boş alanlara hesaplanan hash değerleri yazılarak binary yapının elde edilmesi ve bu yazma işlemlerinin binary olarak yapılması (1006),
- kontrol birimi (3) vasıtasıyla, sertifika binary datası ile gerçek XML datanın uç uca binary olarak birleştirilerek yeni binary yapının oluşturulması (1007) ve

- ❖ kontrol birimi (3) vasıtasıyla, birleştirilen bu binary yapının XML uzantılı dosya (A) olarak depolama birimine (2) yazılması (1008)

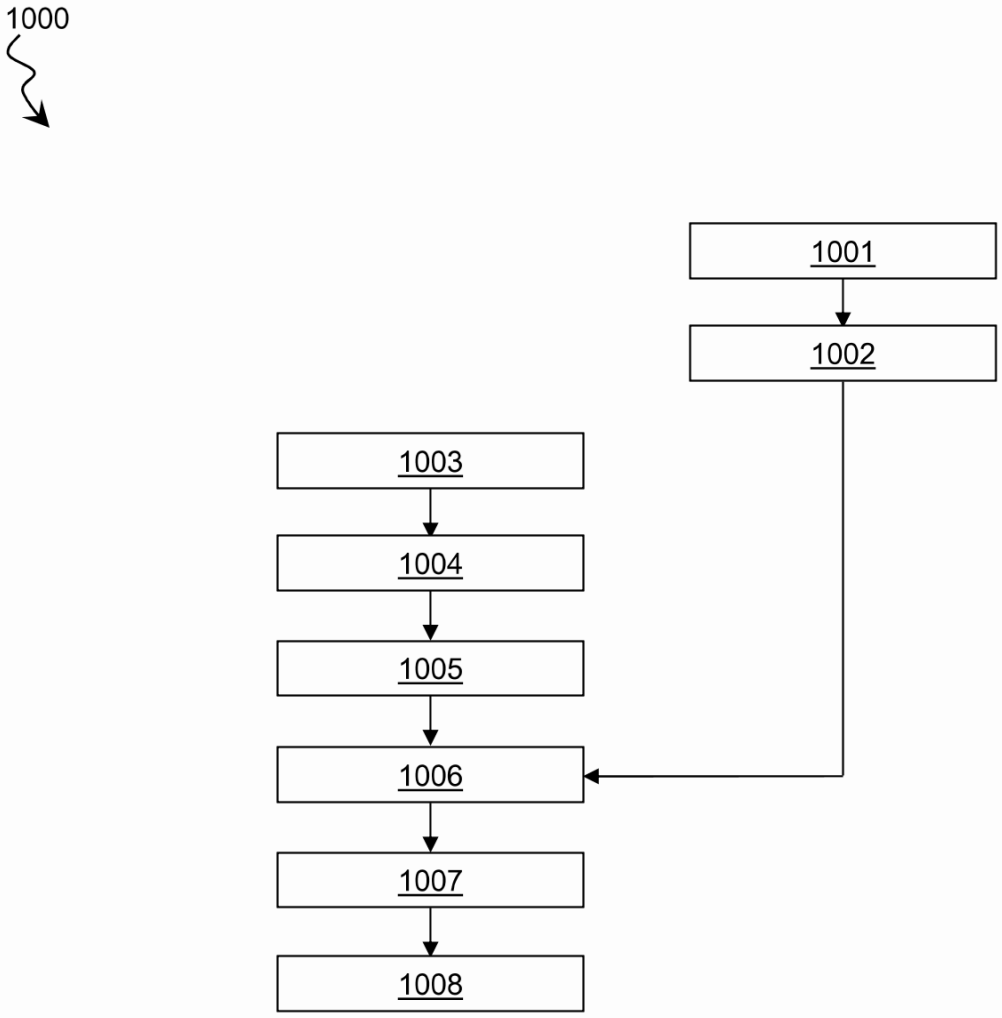
işlem adımlarını içermektedir.

Yöntemde (1000) ilk önce kontrol birimi (3), depolama biriminden (2) sertifika dosyasını (B) okumaktadır. Kontol birimi (3) daha sonrasında, dummy bir test datası ile sertifika hash datalarını elde eder. Kontrol birimi (3) tarafından bu hash dataların içerikleri silinir fakat uzunlukları sabit bırakılır. Bu şekilde, kontrol birimi (3) tarafından, uzunlukları sabit fakat hash datası boş karakterden oluşan binary format elde edilir. Hash datalarının başlangıç ve bitiş adresleri, kontrol birimi (3) tarafından, hafızada saklanır. Bu adım birkez uygulanır; diğer dosyalar (B) için bu adım uygulanmaz. Buradaki amaç; sertifika hash değerlerinin uzunluklarını ve sertifika formatını elde etmek ve diğer XMLler için bir daha çalıştırmamak. Çünkü diğer XML'lerin yapısı da aynıdır. Kontol birimi (3) daha sonrasında, XML dosyasını (A) depolama biriminden (2) binary olarak okur, dosya (A) içerisindeki datanın başlangıç adresini tespit ederek hafızada saklar. Aynı formattaki diğer dosyaların (A) bu başlangıç adresi değişmez ve diğer dosyalarda (A) okunmasına gerek yoktur. Kontol birimi (3), XML dosyasının (A) içerisinde bulunan XML datasını (innerXML), bulunduğu başlangıç adresinden itibaren binary olarak elde eder. Bu binary datadan seritifika hash dataları manuel hesaplanır (digest hash, signature hash gibi). Kontrol birimi (3) sonrasında, daha önce oluşturulan boş sertifika formatını kopyalar ve boş alanlara hesaplanan hash değerlerini yazarak binary yapı elde eder. Bu yazma işlemleri binary olarak yapılır.

Kontrol birimi (3) sertifika binary datası ile gerçek XML datayı uç uca binary olarak birleştirerek yeni binary yapı oluşturur. Birleştirilen bu binary yapı, kontrol birimi (3) tarafından, XML uzantılı dosya (A) olarak depolama birimine (2) yazılır.



Şekil 1



Şekil 2