

QNB eSolutions Elektronik İmza Doğrulama Politikası

Bu belge QNB eSolutions'ın Kayıtlı Elektronik Posta hizmetinde attığı elektronik imzaların nasıl doğrulanacağını tariflenmesi için düzenlenmiştir.

XAdES-A imzaların yapısı

QNB eSolutions KEP delilleri XML formatında olup XML Advanced Electronic Signatures – Archive (XAdES-A) formatındadır. Taban XAdES formatı EPES (Explicit Policy Electronic Signatures) olup, bu taban üzerine iptal bilgileri ve sertifikalar da eklenerek arşiv formatı oluşturulmaktadır.

Doğrulama yöntemi

Kullanılan sertifikalar 5070 sayılı kanuna uygun olarak atılmaktadır. Ek olarak, KEP hizmet sağlayıcısı sertifikasında Bilgi Teknolojileri Kurumunun (BTK) şart koştuğu ekler ve düzenlemeler de vardır (sertifikaya konu kişinin “Subject” tanımında OU alanındaki kullanım amacı metni).

Delil imzaları BTK'nın Haziran 2012 tarihli “ELEKTRONİK İMZA KULLANIM PROFİLLERİ REHBERİ” belgesinde belirtilen 4. tip politikaya (P4) uygundur. Delil imzaları bu profile uygun şekilde doğrulanmalıdır.