



Elektronik Bankacılıkta Uluslararası Yaklaşımlar

Ahmet Türkay VARLI

Bilgi Yönetimi Dairesi / BDDK
Daire Başkanı



Çatı Kurumlar

- Bank for International Settlements (BIS) – Electronic Banking Group of Basel Committee on Banking Supervision

*“Elektronik Bankacılık için Risk Yönetimi İlkeleri” – Temmuz 2003”
(Risk Management Principles for Electronic Banking)*

- European Committee for Banking Standards (ECBS)

*“Elektronik Bankacılık için Güvenlik Kılavuzları: Basel Risk Yönetimi İlkeleri Uygulamaları” – Ağustos 2004
(Security Guidelines for e-Banking: Application of Basel Risk Management Principles)*

Elektronik Bankacılık İçin Risk Yönetim Prensipleri (I)*

Ana Başlıklar:

- Üst Yönetim Gözetimi
- Güvenlik Kontrolleri
- Yasal Risk ve İtibar Riski Yönetimi

Elektronik Bankacılık İçin Risk Yönetim Prensipleri (II)

Üst Yönetim Gözetimi:

- E-Bankacılık Faaliyetleri Üzerinde Etkin Yönetim Gözetimi
- Kapsamlı Güvenlik Kontrol Süreçlerinin Tesis Edilmesi
- Destek Hizmeti Alımına İlişkin Faaliyetlerin Gözetimi, Hizmet Kalitesi ve Diğer Unsurların Takibi

Elektronik Bankacılık İçin Risk Yönetim Prensipleri (III)

Güvenlik Kontrolleri:

- Kimlik Doğrulama
- E-bankacılık İşlemleri İçin İnkâr Edememe ve Güvenilirlik
- Görevler Ayrılığı İçin Uygun Önlemler
- E-bankacılık Sistemleri, Veritabanları ve Uygulamaları İçin Uygun Yetkilendirme
- E-bankacılık İşlemleri, Kayıtları ve Bilgileri İçin Veri Bütünlüğü
- E-bankacılık İşlemleri İçin Denetim İzlerinin (log) Tutulması
- Kritik Banka Bilgileri İçin Gizlilik

Elektronik Bankacılık İçin Risk Yönetim Prensipleri (IV)

Yasal Risk ve İtibar Riski Yönetimi:

- E-bankacılık Hizmetleri İle İlgili Yeterli Açıklama
- Müşteri Bilgilerinin Mahremiyeti
- E-bankacılık Sistemlerinin ve Servislerinin Sürekliliğini Sağlamak Üzere Kapasite, İş Sürekliliği ve İhtimal Planlaması
- Olay Cevap Planı



Ele Alınma Biçimleri

■ Düzenleme

- Mevcut Düzenlemeler Kapsamında Değerlendirme
- Konuya İlişkin Yeni Düzenlemelerin Hazırlanması

■ Kılavuz

Sertifikasyon

(WebTrust, BBBOnline, TrustUK,...)



Sertifikasyon - I

Name	Purpose	Type	Monitoring/ complaints	Owner	Government	Take-up	Cost	Start
WebTrust (HK)	privacy, security, fair trading	audit	follow-up audit at least every 6 months/N	accountancy association	none	neg.	high	Feb 2001
TrustSg (SG)	privacy, fair trading	accredits codes and seals	N N	industry- led	initiation, funding, promotion	v.low	nil	Mar 2001
CaseTrust (SG)	privacy, fair trading	accredits sites	N Y	consumers association	promotion	v.low	low	
E- Confidence (EU)	privacy, fair trading	accredits codes and seals	Y (by code owners)/Y (required for codes)	government	initiation	n/a	n/a	tba
Austrian E- Commerce Quality Mark	privacy, fair trading	accredits sites	Y Y	industry and consumers association	initiation, funding, regulation	med	low	
TrustUK (UK)	privacy, fair trading	accredits codes and seals	Y Y	industry and consumers association	initiation, promotion	low	nil	Jun 2000
Which? WebTrader (UK)	privacy, fair trading	accredits sites	Y Y	consumers association	no	high	nil	Jun 1999

Sertifikasyon - II

Name	Purpose	Type	Monitoring/ complaints	Owner	Government	Take-up	Cost	Start
Online Shopping Trust Mark (JP)	fair trading	accredits sites	N Y	industry-led	no	med	low-med	Apr 2000
IIA Family Friendly ISP (AU)	content	for sites	N N	industry-led	initiation, promotion	low	none (but IIA fee)	Mar 2002
Trustmark (NZ)	fair trading	for sites	N Y	industry-led	support	v.low	low	
BBBOnline (US)	fair trading	for sites	N Y	industry-led	funding, promotion	high	med	
Bobby	Accessibility	accredits sites	N N	non-profit organisation	none	low	nil	
ADMA Code Compliant (AU)	fair trading, (privacy)	for sites	N Y	industry association	no	low	nil	
Verisign's Trusted Commerce	security	accredits sites	N N	industry	no	med	low-med	2002
RSACi	content	for sites	N Y	Industry-led	no	low	v.low	2000



Önemli Konu Başlıkları / Karşılaşılan Riskler

- Kimlik Doğrulama
- İnkâr Edememe
- Güvenlik (Gizlilik)
- Mahremiyet
- Veri Bütünlüğü
- Müşteri Bilgilendirme



Öne Çıkan Korunma Teknikleri

- Çok Faktörlü Kimlik Doğrulama
 - Müşterinin Bildiği Bir Unsur
 - Müşterinin Sahip Olduğu Bir Unsur
 - Müşterinin Biyolojik Tekil Bir Özelliği
- E-imza
- İletilen Verinin Şifrelenmesi



Karşılaşılan Güçlükler

- Bazı Tekniklerin Kullanım Alt Yapısının Oluşmamış Olması (E-İmza)
- Teknolojinin Gelişen ve Değişen Yapısı
- Genel Erişime Açık Ortam
- Kullanıcı Bilinçlendirme



BDDK Çalışmaları

- Bankalarda Bilgi Sistemlerinin Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ
- İnternet Bankacılığı



İLGİNİZ İÇİN TEŞEKÜRLER

SORULAR