# Informatieclassificatie en behandelingsspecificatie voor derden

## Introductie

Niet alle informatie heeft dezelfde waarde of is even gevoelig en het classificeren ervan helpt ons uit te werken hoe het beschermd zou moeten worden, toont onze betrokkenheid bij die bescherming en helpt ons het efficiënt te behandelen.

Wij hanteren vier classificatieniveaus:

- Openbaar
- Intern
- In vertrouwen
- In het striktste vertrouwen

De onderstaande tabel geeft inzicht in de soorten informatie die onder elk van deze vier categorieën vallen.

Alle BT-data wordt standaard geclassificeerd als "In vertrouwen" tenzij anders aangegeven.

Neem contact op met uw BT-contactpersoon beveiliging als u er niet zeker van bent onder welke categorie bepaalde informatie valt.

| Classificatie | Overzicht beschrijving | Voorbeelden |
|---|---|---|
| **Openbaar – Cat. 1** | Openbare informatie is informatie die beschikbaar is voor personen zowel binnen als buiten BT. | • Reclamecampagnes.<br>• Generieke mededelingen die al zijn opgenomen in het publieke domein (b.v. PR-mededelingen, openbare artikelen over BT)<br>• Publiekelijk beschikbare commerciële informatie zoals gepubliceerde prijzen of aanbiedingen |
| **Intern – Cat. 2** | BT-informatie die beschikbaar is voor BT-medewerkers en andere personen die toegang hebben tot het informatienetwerk van BT, waarbij een dergelijke toegang resulteert in een minimaal bedrijfsrisico voor BT.<br><br>Interne informatie kan informatie zijn die onderhevig is aan algemene geheimhoudingsplicht (b.v. e-mails over de normale bedrijfsvoering, rapportages of contractuele documenten) mits die informatie niet voldoende commercieel gevoelig is om de hieronder beschreven verhoogde bescherming te vereisen. | • Interne nieuwsbrieven zoals BT News<br>• FixIt artikelen<br>• Algemene niet-gevoelige e-mails (b.v. zonder commerciële informatie of beperkte persoonsgegevens zoals gespecificeerd in de linkerkolom die is opgenomen in de tekst van de e-mail) |
| **In vertrouwen – Cat. 3** | Informatie met de categorie "In vertrouwen" is informatie die beperkt is tot een specifiek publiek en waarvan de onbevoegde openbaarmaking schade kan toebrengen aan de reputatie van BT of waarvan de openbaarmaking mogelijk schadelijk kan zijn voor de personen wiens informatie het betreft (b.v. de meeste persoonsgegevens van medewerkers | • Logdata van het systeem;<br>• Commercieel gevoelige verkoop- en marketingdata;<br>• Lokale bedrijfsplannen;<br>• De meeste persoonsgegevens; en<br>• Risicodata.<br>• Alle persoonsgegevens (zoals gedefinieerd onder de voorwaarde genaamd |

| | | |
|---|---|---|
| | of klanten). Het "need-to-know" principe moet worden toegepast voor vertrouwelijke informatie.<br><br>**Verzameling van meerdere "In vertrouwen"-documenten**<br><br>Indien u een verzameling documenten met de categorie "In vertrouwen" op een locatie bewaard, dan kan het zijn dat de classificatie moet worden verhoogd en dit kan leiden tot de herclassificatie van individuele documenten tot "In het striktste vertrouwen" of de noodzaak tot aanvullende beveiligsmaatregelen om de locatie veilig te stellen als:<br>• De documenten samen uitzonderlijke schade kunnen veroorzaken voor BT als deze zouden uitlekken; of<br>• Deze een aantrekkelijk doelwit kunnen vormen indien gebruikt met andere data-itemcombinaties. | "**Bescherming van Informatie**") tenzij deze hieronder zijn geclassificeerd als "In het striktste vertrouwen". |
| **In het striktste vertrouwen – Cat 4** | Informatie of data met de categorie "In het striktste vertrouwen" heeft circuleert in een gedefinieerde en kleine oplage; het "need-to-know" principe wordt streng toegepast (u moet weten wie er kopieën heeft en wie er toegang heeft). Onbevoegde openbaarmaking kan uitzonderlijke schade veroorzaken voor BT. U moet zorgvuldig afwegen of bepaalde informatie "In het striktste vertrouwen" is want dit vereist de strengste veiligheidscontroles. | • Details over bankrekeningen<br>• Authenticatiegegevens moeten als "In het striktste vertrouwen" worden behandeld.<br>• Wachtwoorden voor computers. Wachtwoorden moeten worden opgeslagen en beveiligd in overeenstemming met de cryptografiespecificaties van BT<br>• Financiële boekhoudkundige data onder embargo tot de publicatie van het jaarverslag<br>• Strategische bedrijfsplannen, concurrentiestrategie, nieuwe strategische producten en nieuw marketingbeleid<br>• Zeer gevoelige beoordelingen van een concurrent, partner of contractant<br>• Gevoelige HR-informatie die een aanzienlijk aantal werknemers schade kan berokkenen<br>• Details over een grote overname, alliantie, afsplitsings- en fusieplannen<br>• Details over aanzienlijke kwetsbaarheden in het netwerk<br>• Beveiligingscodes van klanten, masterencryptiecodes, belangrijke berekeningen, details over een transactie, rekening of audit<br>• Auditrapporten of bevindingen die data bevatten van ernstige tekortkomingen/kwetsbaarheden in de praktijken of processen van BT |

## Hoe ga ik om met de data?

Informatie moet worden behandeld volgens het classificatieniveau zodat het naar behoren is beveiligd, of dit nu op een computer is, wordt gedeeld op een netwerk, op schrift is gesteld of gesproken.

Wij hebben regels voor het omgaan met data en informatie.

- **Gesproken en multimedia** b.v. praten, sociaal netwerken, SMS-en of Skypen
- **Papieren documenten** b.v. printen, posten of opruimen
- **Elektronische documenten** b.v. opslaan, e-mailen, delen, verwijderen
- **In applicaties of systemen** b.v. datacentra

Wij hebben ook afzonderlijke richtlijnen op het niveau en soort encryptie dat we verwachten te gebruiken voor de bescherming van informatie (onze "encryptiestandaard").

## Omgaan met gesproken & multimedia data

| Ref. | Wat wilt u doen? | Classificatie | Verwerkingsvereisten | Reden |
|---|---|---|---|---|
| **HSM10** | Ik wil informatie plaatsen op sociale media/netwerksites – b.v. persoonlijk Twitteraccount | Openbaar | U mag niet bijdragen aan sites of online uitspraken plaatsen die redelijkerwijs kunnen worden toegeschreven aan de opvattingen van BT of die lasterlijk zijn voor BT en schade kunnen berokkenen aan het merk en de reputatie van BT. | Onbevoegde openbaarmaking van informatie of een persoonlijk commentaar kan ons merk schaden |
| | | Intern | Niet toegestaan | |
| | | In vertrouwen | Niet toegestaan | |
| | | In het striktste vertrouwen | Niet toegestaan | |
| **HSM20** | Ik wil iets bespreken of presenteren middels een interne conferentie of bericht | Intern | U kunt Live Meeting, WebEx, Webjoin en Lync/Skype for Business gebruiken | Interne data kan worden gezien door personen die zijn uitgenodigd voor de meeting |
| | | In vertrouwen | U kunt Live Meeting, WebEx, Webjoin en Lync/Skype for Business gebruiken | Vertrouwelijke data kan worden gezien door personen die zijn uitgenodigd voor de meeting |
| | | In het striktste vertrouwen | • U kunt Lync/Skype for Business gehost door BT gebruiken<br>• U moet verifiëren wie deelneemt aan de conferentie<br>• U moet de conferentiebijeenkomst vergrendelen zodat niemand anders zich kan aansluiten | Lync/Skype for Business codering volgens de onderstaande data van encryptiestandaard |
| **HSM30** | Ik wil iets bespreken via een externe live chat, bijvoorbeeld op een ondersteunende leverancierssite zoals Cisco | Openbaar | Gesprekken moeten worden beperkt tot "openbare informatie" die vrij toegankelijk is op onze website | Om onbevoegde openbaarmaking van informatie te voorkomen |
| | | Intern | Niet toegestaan | |
| | | In vertrouwen | Niet toegestaan | |
| | | In het striktste vertrouwen | Niet toegestaan | |

| | | | | |
|---|---|---|---|---|
| **HSM40** | Ik wil iets persoonlijk/in een telefoongesprek met iemand bespreken | Intern | Zorg ervoor dat het gesprek niet kan worden gehoord door een persoon die niet werkt voor of namens BT | Om onbevoegde openbaarmaking van informatie te voorkomen |
| | | In vertrouwen | Als "Intern" en<br>• Controleer de identiteit van de persoon waarmee u praat en bevestig dat zij een "need-to-know'" status hebben alvorens iets vertrouwelijks te bespreken<br>• Verzeker u ervan dat een contract is afgesloten met derden alvorens het gesprek te beginnen, indien van toepassing (NB: Alvorens het volledige of een deel van het contract toe te wijzen of uit te besteden aan een 3de partij moet u de voorafgaande schriftelijke toestemming van BT hebben)<br>• Zorg dat het gesprek niet kan worden afgeluisterd<br>• Laat geen "in vertrouwen"-informatie achter op voicemailsystemen | Om vertrouwelijke informatie te beschermen en om er zeker van te zijn dat deze informatie is beperkt tot de personen die dit moeten weten |
| | | In het striktste vertrouwen | Als "in vertrouwen" en<br>• Beperk "In het striktste vertrouwen"-informatie tot een absoluut minimum | |
| **HSM50** | Ik wil een bericht/informatie via SMS/MMS sturen aan alle partijen (intern & extern) | Openbaar | De inhoud van het bericht moet beperkt blijven tot "openbare informatie" die op onze website beschikbaar is | Om onbevoegde openbaarmaking van informatie te voorkomen |
| | | Intern | Geen bijzondere verwerkingsvereisten | |
| | | In vertrouwen | Zorg dat het bericht uitsluitend wordt verstuurd aan de juiste personen en het onderstaande mag niet worden vermeld:<br>• Betaalkaartinformatie<br>• Bankgegevens<br>• Wachtwoord details | Deze 3 soorten gegevens zijn "In het striktste vertrouwen" |
| | | In het striktste vertrouwen | Niet toegestaan | |

# Omgaan met papieren documenten

| Ref | Wat wilt u doen? | Classificatie | Verwerkingsvereisten | Reden |
|---|---|---|---|---|
| **HPD10** | Ik wil werken aan informatie op papier in de bedrijfsruimte van een 3de partij of thuis | Intern | U moet uw bureau leegmaken als u niet aan uw bureau zit | Om accidentele openbaarmaking te voorkomen |
| | | In vertrouwen | Als "Intern" en<br>• Als u niet aan de documenten werkt, plaats deze dan uit het | |

| | | | | |
|---|---|---|---|---|
| | | | zicht en bewaar ze achter een slot. | |
| | | In het striktste vertrouwen | Als "In vertrouwen" | |
| **HPD20** | Ik wil printen | Intern | • Controleer of u het document naar de juiste printer stuurt<br>• Laat geen documenten achter in de printerlade | Om accidentele openbaarmaking te voorkomen |
| | | In vertrouwen | Als "Intern" en<br>• Gebruik een printer met gecontroleerde toegang, een printer die is aangesloten op een PC of een printer in een ruimte met toegangscontrole | |
| | | In het striktste vertrouwen | Als "in vertrouwen" | |
| **HPD30** | Ik wil een printer gebruiken die zich niet bevindt in een leveranciersgebouw of bij mij thuis (b.v. in een gebouw van een derde partij, een hotel, enz.) | Intern | Dit is gewoonlijk niet toegestaan want printers hebben een geheugen en data kan hieruit worden opgehaald.<br><br>Gebruik uw gezond verstand – wilt u echt dat andere personen deze informatie zien? | Data en informatie kunnen worden opgehaald uit het geheugen van een printer |
| | | In vertrouwen | Niet toegestaan | |
| | | In het striktste vertrouwen | Niet toegestaan | |
| **HPD40** | Ik wil papieren informatie meenemen buiten mijn werkplaats | Intern | Draag deze in een ondoorzichtige map of tas | Om de informatie te beschermen tegen accidentele openbaarmaking |
| | | In vertrouwen | Als "Intern" en<br>• Klant- en/of betaalgegevens mogen niet worden meegenomen uit leverancierskantoren | |
| | | In het striktste vertrouwen | Als "In vertrouwen" | |
| **HPD50** | Ik wil papieren informatie delen met of sturen naar interne partijen | Intern | • Plaats in een envelop en gebruik de interne post. | Beschermt tegen terloopse observatie |
| | | In vertrouwen | • Schrijf niet "In vertrouwen" op de buitenste envelop.<br>• Win advies in bij uw juridische team als de informatie valt onder wettelijk privilege. | Voorkomt dat terloopse waarnemers weten dat de inhoud "In vertrouwen" is. Aangetekende verzending bestaat uit een bewijs van posten, handtekening voor ontvangst en online bevestiging van de aflevering |
| | | In het striktste vertrouwen | • Gebruik 2 enveloppen en verstuur deze met gebruikmaking van een "tracked" levering<br>• Schrijf niet "In het striktste vertrouwen" op de buitenste envelop | Voorkomt dat terloopse waarnemers weten dat de inhoud "In het striktste vertrouwen" is. Aangetekende verzending bestaat uit een bewijs van |

| | | | | |
|---|---|---|---|---|
| | | | • Krijg toestemming van de eigenaar van het document om de papieren versie te delen<br>• Deel het document bij voorkeur persoonlijk met bevoegde bij naam bekende personen<br>• Associeer kopieën met personen door deze te voorzien van een watermerk met een naam of nummer (indien beschikbaar)<br>• Indien verloren, rapporteer een beveiligingsincident | posten, handtekening voor ontvangst en online bevestiging van de aflevering |
| **HPD60** | I wil een papieren document delen met of sturen naar externe partijen | Intern<br>In vertrouwen<br>In het striktste vertrouwen | Zorg dat er een contract met relevante 3de partijen volgens HSM40. Daarna zijn de vereisten hetzelfde als voor delen met interne partijen | Zie HPD50 |
| **HPD70** | Ik wil een fax sturen | Intern | Zorg dat een fax voorblad wordt gebruikt voor de inhoud van de pagina(s) | Om accidentele openbaarmaking te voorkomen |
| | | In vertrouwen | • U moet een voorblad sturen met een testpagina en vervolgens contact opnemen met de ontvanger om de ontvangst te bevestigen alvorens de inhoud te faxen<br>• Win advies in bij uw juridische team als de informatie valt onder wettelijk privilege | Om te voorkomen dat onbevoegde personen informatie krijgen |
| | | In het striktste vertrouwen | Niet toegestaan | |
| **HPD80** | Ik wil papieren informatie weggooien | Intern | U moet<br>• deze versnipperen of<br>• deze plaatsen in een documentenbak waar het niet makkelijk kan worden uitgehaald | Algemene afval- en/of recyclingbakken zijn geen veilige manieren van weggooien |
| | | In vertrouwen | U moet de informatie versnipperen tot stukjes van minimaal ≤ 160MM² en tot normale stroken met een breedte van ≤ 2MM b.v. 2X15 mm. | Om vertrouwelijke informatie te beschermen tegen openbaarmaking |
| | | In het striktste vertrouwen | U moet de informatie versnipperen tot stukjes van minimaal ≤ 160MM² en tot normale stroken met een breedte van ≤ 2MM b.v. 2X15 mm door gebruik te maken van een kruiselings snijdende versnipperaar | Om "In het striktste vertrouwen"-informatie te beschermen tegen openbaarmaking |

# Omgaan met elektronische documenten

| Ref. | Wat wilt u doen? | Classificatie | Verwerkingsvereisten | Reden |
|---|---|---|---|---|
| **HED10** | Ik wil elektronische informatie opslaan op mijn zakelijke laptop/PC | Intern | Volledige schijfencryptie gebruikt volgens de onderstaande encryptiestandaard. | Dit converteert informatie in een onleesbare code |

| | | | | |
|---|---|---|---|---|
| | | | | die niet makkelijk kan worden ontcijferd door onbevoegde personen. |
| | | In vertrouwen | Volledige schijfencryptie gebruikt volgens de onderstaande encryptiestandaard. | |
| | | In het striktste vertrouwen | Volledige schijfencryptie gebruikt volgens de onderstaande encryptiestandaard. | |
| **HED20** | Ik wil mijn documenten opslaan op SharePoint of een ander documentmanagementsysteem dat NIET is gehost in de cloud of met internetservices | Intern | • Gebruik toestemmingsniveaus en -groepen toegangscontrole op basis van rol op te zetten. Deze moet worden ingesteld op niet meer dan het minimum om personen hun werk te laten doen<br>• Controleer de toegangscontroles elk jaar | Beperkt toegang en/of recht tot bewerking tot diegenen die dit moeten weten |
| | | In vertrouwen | Als "Intern" en<br>• Documenteer het proces om personen aan rollen toe te wijzen.<br>• De rollen en personen die hieraan zijn toegewezen moeten elke 90 dagen worden gecontroleerd<br>• Documenten moeten zijn gecodeerd volgens de onderstaande encryptiestandaard | |
| | | In het striktste vertrouwen | Als "Intern" en<br>• Documenteer het proces om personen aan rollen toe te wijzen.<br>• De rollen en personen die hieraan zijn toegewezen moeten elke 90 dagen worden gecontroleerd<br>• Documenten moeten zijn gecodeerd volgens de onderstaande encryptiestandaard | |
| **HED30** | Ik wil elektronische informatie opslaan in de cloud of met internetservices zoals Google Docs, GitHub, btcloud.bt.com, Dropbox, Pastebin, Facebook enz. | Intern | Niet toegestaan. | Internetservices verhogen het risico op onbevoegde toegang tot de informatie |
| | | In vertrouwen | Niet toegestaan. | |
| | | In het striktste vertrouwen | Niet toegestaan. | |
| **HED40** | Ik wil elektronische informatie opslaan op verwijderbare media, b.v. een geheugenstick. | Intern | • USB-apparaten moeten zijn gecodeerd volgens de onderstaande encryptiestandaard | Verwijderbare media kan makkelijker worden verloren of gestolen dan |

| | | | | |
|---|---|---|---|---|
| | | | In geen enkel geval mogen persoonsgegevens worden opgeslagen op deze apparaten tenzij gecodeerd volgens de onderstaande encryptiestandaard. | een hele computer en dus is het risico groter dat onbevoegde personen toegang krijgen tot de data. Om de informatie te beschermen moet deze worden geconverteerd naar een onleesbare code die niet makkelijk kan worden ontcijferd door onbevoegde personen |
| | | In vertrouwen | Als "Intern" | |
| | | In het striktste vertrouwen | Als "Intern" | |
| **HED50** | Ik wil elektronische documenten of BT-informatie opslaan op mijn persoonlijke laptop of apparaat | Intern | Niet toegestaan | Onbevoegde personen kunnen eventueel toegang krijgen tot BT-data, zeker als het apparaat wordt verloren, gestolen of ingewisseld voor een nieuwer model. |
| | | In vertrouwen | Niet toegestaan | |
| | | In het striktste vertrouwen | Niet toegestaan | |
| **HED60** | Ik wil elektronische documenten of informatie versturen naar mijn persoonlijke e-mailadres | Intern | Niet toegestaan | Om openbaarmaking aan onbevoegde personen te voorkomen |
| | | In vertrouwen | Niet toegestaan | |
| | | In het striktste vertrouwen | Niet toegestaan | |
| **HED70** | Ik wil automatisch doorsturen naar een e-mailadres | Intern | Niet toegestaan | Toegang tot de data kan worden verkregen door onbevoegde personen als de e-mailaccount, ISP of internetverbinding is gecompromitteerd |
| | | In vertrouwen | Niet toegestaan | |
| | | In het striktste vertrouwen | Niet toegestaan | |
| **HED80** | | Intern | Geen bijzondere vereisten | |

| | | | | |
|---|---|---|---|---|
| | Ik wil *intern* elektronische informatie delen of versturen via e-mail | In vertrouwen | • Maak duidelijk dat de e-mail "In vertrouwen" is<br>• Gebruik gevoeligheidsinstellingen om de e-mail te markeren als "In vertrouwen"<br>• Stel de toestemming idealiter in op "Niet doorsturen"<br>• Win advies in bij uw juridische team als de informatie valt onder "wettelijk privilege"<br>• | Om de controle te behouden over vertrouwelijke informatie |
| | | In het striktste vertrouwen | Als "In vertrouwen" plus<br>• Gebruik beveiligde e-mail om te versturen<br>• Indien beveiligde e-mail niet mogelijk is, dan moet u het bestand voor verzending coderen volgens de onderstaande encryptiestandaard<br>• Stel de toestemming in op "Niet doorsturen" | Om de informatie te beschermen terwijl via de netwerken gedeeld wordt |
| **HED90** | Ik wil *extern* elektronische informatie delen of versturen via e-mail | Intern | U kunt alleen informatie sturen naar een externe partij als er een contract is volgens HSM40 | Om de controle te behouden over vertrouwelijke informatie |
| | | In vertrouwen | Als "Intern" en<br>• Codeer volgens de onderstaande encryptiestandaard<br>• Bevestig dat u de informatie stuurt naar het juiste e-mailadres<br>• Win advies in bij uw juridische team als de informatie valt onder "wettelijk privilege" | |
| | | In het striktste vertrouwen | Als "In vertrouwen" | |
| **HED120** | Ik wil een back-up maken van elektronische documenten van BT | Intern | • U moet uw documenten opslaan op de netwerkdrives van de leverancier of het documentmanagementsysteem van de leverancier volgens HED030.<br>• De documenten waarvoor u een back-up heeft gemaakt moeten op hetzelfde niveau worden beschermd als op de netwerkdrive, SharePoint.<br>• Als u verwijderbare media gebruikt, dan moet het apparaat zijn gecodeerd volgens de onderstaande encryptiestandaard. | Back-ups moeten hetzelfde niveau van classificatie & bescherming hebben als de originele data |

| | | | | |
|---|---|---|---|---|
| | | In vertrouwen | Als "Intern" en<br>• Codeer het document volgens de onderstaande encryptiestandaard alvorens een back-up te maken | |
| | | In het striktste vertrouwen | Als "In vertrouwen" | |

# Omgaan met systeem & applicatie data

| Ref. | Wat wilt u doen? | Classificatie | Verwerkingsvereisten | Reden |
|---|---|---|---|---|
| **HSADE** | Ik wil elektronische data & informatie opslaan en bewerken die wordt bewaard in een datacentrum of op een systeemserver | Intern | Geen bijzondere vereisten indien het voldoet aan alle bovenstaande toepasselijke vereisten voor het opslaan van data voor deze classificatie. | |
| | | In vertrouwen | U moet de vereisten voor externe datahosting door derden opvolgen http://www.selling2bt.com/working/ThirdPartySecurity standards/index.htm | |
| | | In het striktste vertrouwen | Als "In vertrouwen" plus<br><br>Om bankrekeninggegevens te beschermen, aangezien deze bijzonder gevoelig zijn, zijn de volgende controles van toepassing. Deze hebben prioriteit boven enige andere toepasselijke controles in deze beveiligingsspecificatie.<br><br>1. Bankrekeningen moeten worden omgezet naar tokens voor individuen (persoonlijke bankrekeningen van klanten of BT-werknemers). Dit is uitgezonderd de eigen bankrekeninggegevens van BT en de bankgegevens van de verschillende BT-rechtspersonen.<br><br>2. Indien een applicatie alleen zakelijke bankrekeningen bewaard, dan kan de 3de partij de discussie aangaan (gebaseerd op tijd, kosten, bron, aantal rekeningen en aantal gebruikers met toegang tot de applicatie, enz.) of BT aanvankelijk een op encryptie gebaseerde oplossing zal accepteren. | |

| | | | | |
|---|---|---|---|---|
| | | | Als een op encryptie gebaseerde oplossing wordt overeengekomen, dan zal BT de beslissing beoordelen als alle bankrekeningen zijn beschermd om te bepalen of het adequaat is om verder te gaan. Dit zal worden beïnvloed door de dreigingsniveaus en risicobereidheid van het bedrijf als geheel.<br><br>3. Als de daadwerkelijke bankrekeninggegevens worden getoond aan een vertegenwoordiger als onderdeel van een bedrijfsproces (b.v. om te verifiëren dat we de juiste rekening hebben om te factureren, of als communicatie plaatsvindt met een klant, b.v. via e-mail of op een factuur) moeten we alleen de laatste 4 cijfers van de bankrekening tonen (zogenaamde gemaskeerde bankrekeninggegevens).<br><br>4. Indien er een noodzaak bestaat tot volledige toegang tot de bankrekening (b.v. om een credit of debet verzoek van een bank in te willigen), dan moeten de gegevens worden "de-tokenised" of gedecodeerd en dan worden doorgegeven aan de bank met gebruikmaking van een gecodeerd transportmechanisme dat voldoet aan het BT-beveiligingsbeleid. Onmiddellijk na gebruik moeten de gedecodeerde of "de-tokenised" bankgegevens op een veilige manier worden gewist. | |

# Encryptiestandaarden

## Algemene cryptografie controles

| Ref | Controle | Reden |
|---|---|---|
| **C1.10** | De huidige cryptografische bibliotheken moeten worden gebruikt | Cryptografische bibliotheken worden regelmatig bijgewerkt. Aanvullend op het updaten van softwarepakketten in lijn met de richting van de leverancier, moeten cryptografische pakketten regelmatig worden beoordeeld en bijgewerkt. |
| **C1.20** | Gebruik alleen goedgekeurde coderingssuites die voldoen aan de industriestandaard voor encryptie. B.v. voor TLS SSLv2 | Niet-goedgekeurde coderingen kunnen kwetsbaarheden introduceren |
| **C1.30** | De laatste versie van TLS moet worden gebruikt voor nieuwe plaatsingen. SSL V1,2 & 3 mogen niet worden gebruikt | Eerdere versies, tot en met TLS1.0, worden niet langer beschouwd als veilig |
| **C1.40** | Perfect forward secrecy moet worden geactiveerd | Perfect forward secrecy-algoritmen voorkomen dat onderschepte berichten worden gedecodeerd zelfs als de authenticatie van de persoonlijke sleutel in de toekomst wordt aangetast |
| **C1.50** | Zelfgetekende certificaten mogen niet worden gebruikt | Zelfgetekende certificaten doen het voordeel van eindpunt-authenticatie teniet en verlagen ook aanzienlijk het vermogen van een individu om een man-in-the-middle aanval te signaleren. |
| **C1.60**<br><br>**GTS2.370** | Een certificeringsautoriteit die voldoet aan de industriestandaard moet worden gebruikt voor certificaatbeheer. B.v. Verisign | Om een inventarisatie bij te houden van certificaten die zijn uitgegeven vanwege kwetsbaarheden en vervallen van het certificaat |
| **C1.70** | Wachtwoorden moeten worden beschermd door gebruik te maken van een niet-omkeerbare | Opgeslagen wachtwoordbestanden kunnen worden onttrokken en als zodanig moeten alle gegevens |

| | | |
|---|---|---|
| | eenzijdige wiskundige functie (b.v. Hashing algoritme) met een unieke willekeurige factor (Salt) per wachtwoord.<br><br>NB. Salt is willekeurige data die wordt gebruikt als een aanvullende invoer op een eenzijdige functie die een wachtwoord of wachtzin "hashed". | worden beschermd om het terughalen van wachtwoorden met duidelijke tekst te voorkomen |
| **C1.80** | Beschermde wachtwoorden volgens C1.70 moeten buiten de configuratiebestanden van een systeem worden opgeslagen en hebben een toegangscontrole geïmplementeerd zodat alleen de juiste bevoorrechte gebruikers de inhoud kunnen lezen of kopiëren. | Het mag nooit mogelijk zijn om beschermde wachtwoorden te achterhalen door middel van het doorlopen van de map, SNMP-loop, configuratielozing of ander mechanisme, die pogingen tot offline inbreken kunnen toestaan. |

## Technische cryptografie implementatie

| **SSL/TLS-protocollen** | |
|---|---|
| **Kan gebruiken** | **Niet gebruiken** |
| TLSv1.3 (tbc – Beschikbaar in OpenSSL na 5 april). | SSLv3.0 |
| TLSv1.2 | SSLv2.0 |
| TLSv1.1 | |
| TLS v1.0* | |

***** TLSv1.0 heeft het einde van de levensduur bereikt en kan op elk moment worden afgeschreven vanwege bekende problemen. Om reden van naleving (bijvoorbeeld PCI-DSS) van protocollen kunnen TLSv1.0 en TLSv1.1 worden uitgezet. Alle ontwikkelaars zouden er klaar voor moeten zijn om dit protocol uit te schakelen middels configuratie.

| **Sleutelgroottes** | | | |
|---|---|---|---|
| | **Symmetrisch** | **Asymmetrisch** | **Elliptische boog** |
| **Brownfield** | ≥ 112 bits | ≥ 2048 bits | ≥ 224 bits |
| **Greenfield** | ≥ 128 bits | ≥ 3072 bits | ≥ 384 bits |

| **Sleuteloverdracht** | |
|---|---|
| **Kan gebruiken** | **Niet gebruiken** |
| ECDHE (Kortstondige (tijdelijke sleutel) Diffie-Hellman sleuteloverdracht (sleutels niet gebaseerd op certificaten)) | kRSA (RSA sleuteloverdracht) |
| | kDHr (Diffie-Hellman sleuteloverdracht met RSA sleutel) |
| | kDHd (Diffie-Hellman sleuteloverdracht met DSA sleutel) |
| | kSRP (Beveiligd extern wachtwoord (SRP) sleuteloverdracht)<br>kADH (Anonieme Diffie-Hellman sleuteloverdracht) |
| | kPSK (Vooraf gedeelde sleutel sleuteloverdracht) |

"Perfect forward" beveiliging moet zijn gebaseerd op plaatselijk geconfigureerde of gegenereerde Diffie-Hellman Groep waarden die "veilige" priemgetallen bevatten.

**Diffie-Hellman parameters**

| **Diffie-Hellman parameters** | |
|---|---|
| **Kan gebruiken** | **Niet gebruiken** |

| | |
|---|---|
| **3072-bit Diffie-Hellman Groep (beste – moet plaatselijk worden gegenereerd).** | De standaardwaarden van de server (genereer plaatselijk uw eigen waarden) |
| **2048-bit Diffie-Hellman Groep (nadert einde levensduur – moet plaatselijk worden gegenereerd).** | |

| **Authenticatie** | |
|---|---|
| **Kan gebruiken** | **Niet gebruiken** |
| aRSA (RSA authenticatie) | aNULL (Geen authenticatie) |
| aECDSA (Elliptische boog digitale handtekening algoritme authenticatie) | aDSS (DSS authenticatie) |
| | aECDH (Elliptische boog Diffie-Hellman) |
| | aDH (Diffie-Hellman) |
| | aDSA (Digitale handtekening algoritme) |
| | aPSK (Vooraf gedeelde sleutel) |
| | aSRP (Beveiligd extern wachtwoord) |

| **Versleuteling/Encryptie** | |
|---|---|
| **Kan gebruiken** | **Niet gebruiken** |
| AES 256 GCM (Rijndael (geavanceerde encryptiestandaard) - Galois teller modus) | eNULL (Geen encryptie) |
| AES 128 GCM (Rijndael (geavanceerde encryptiestandaard) - Galois teller modus) | DES (DES encryptie) |
| CHACHA20/POLY1305 (256) | 3DES (3DES encryptie) |
| AES 256 CCM (Rijndael (geavanceerde encryptiestandaard) - (teller modus met CBC-Mac) | RC4 (RC4 encryptie) |
| AES 128 CCM (Rijndael (geavanceerde encryptiestandaard) - (teller modus met CBC-Mac) | RC2 (RC2 encryptie) |
| AES 256 CBC (Rijndael aaneenschakeling versleutelingsblok) – nadert einde levensduur. | IDEA (IDEA encryptie) |
| AES 128 CBC (Rijndael aaneenschakeling versleutelingsblok) – nadert einde levensduur. | Seed (Seed encryptie) |
| | Camellia (Camellia encryptie) |
| | ARIA (ARIA encryptie) |

| **MAC Digest algoritme** | |
|---|---|
| **Kan gebruiken** | **Niet gebruiken** |
| AEAD (Geauthenticeerde aanvullende encryptie data) | MD5 (MD5 Hash functie) |
| SHA512 (SHA2-familie - SHA512 Hash functie) | SHA1 (SHA1 Hash functie) |
| SHA384 (SHA2-familie - SHA384 Hash functie) | SHA (pseudoniem voor SHA1) |
| SHA256 (SHA2-familie - SHA256 Hash functie) | |