

**BDK**

Índice

[1. BDK 3](#_Toc44147200)

[2. BDK Type 2 (“BDK-2”): 3](#_Toc44147201)

[3. BDK Type 3 (“BDK-3”): 3](#_Toc44147202)

[4. BDK Type 4 (“BDK-4”): 4](#_Toc44147203)

[5. Rease Notes 5](#_Toc44147204)

# BDK

A chave do tipo BDK, Base Derivation Key, como o próprio nome diz, é uma chave de derivação, ou seja, ela serve para derivar/criar outras chaves a partir dela. A partir do padrão DUKPT (X9.24-1:2009) temos dois métodos diferentes para a derivação de chaves, o método **bidirecional** e o **unidirecional**.

Basicamente o método bidirecional utiliza uma única chave para proteger dados do terminal para o host e vice-versa, enquanto o unidirecional utiliza duas chaves, uma para proteger os dados do terminal para o host e outra para proteger os dados do host para o terminal.

A BDK tipo 1 e 3 suportam o método bidirecional.

A BDK tipo 2 e 4 suportam o método unidirecional.

Porém cada tipo de BDK serve para um proposito, por exemplo, uma BDK do tipo 1 é usado em três tipos de chaves bidirecionais, uma delas é chaves para criptografia de PIN. Já uma BDK do tipo 3 usa a variante “Pin encryption” para a derivação, porém, só pode ser usado para executar operações de criptografia de dados.

**BKD Type 1 (“BDK-1”):**

Três tipos de chaves bidirecionais podem ser derivados de um BDK-1:

> Chaves de criptografia de PIN

> Chaves de autenticação de dados (MAC)

> Chaves de criptografia de dados

# BDK Type 2 (“BDK-2”):

Cinco tipos de chaves unidirecionais podem ser derivados de um BDK-2:

> Chaves de criptografia de PIN (para mensagens do terminal para o adquirente)

> Chaves de autenticação de dados (MAC) (para mensagens do terminal para o adquirente)

> Chaves de autenticação de dados (MAC) (para mensagens do adquirente para o terminal)

> Chaves de criptografia de dados (para mensagens do terminal para o adquirente)

> Chaves de criptografia de dados (para mensagens adquirentes para o terminal)

# BDK Type 3 (“BDK-3”):

Um tipo de chave bidirecional pode ser derivado de um BDK-3:

> Chave de criptografia de dados

# BDK Type 4 (“BDK-4”):

Cinco tipos de chaves unidirecionais podem ser derivados de um BDK-4:

> Chaves de criptografia de PIN (para mensagens do PSP para o adquirente)

> Chaves de autenticação de dados (MAC) (para Mensagens do PSP para adquirente)

> Chaves de autenticação de dados (MAC) (para mensagens do adquirente para o PSP)

> Chaves de criptografia de dados (para mensagens do PSP para o adquirente)

> Chaves de criptografia de dados (para mensagens do adquirente para a PSP)

\***Note: PSP = Payment Service Provider**\*

# Rease Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Caio Ferreira | Primeira versão | 12/05/2020 |
|  |  |  |