

RSA® Conference 2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: HT-R05

Token Theft: Hip Kids Are Doing It

Now what are we going to do about it?

Alex Weinert

Director of Identity Security
Microsoft Corporation
@Alex_T_Weinert

Anna Barhudarian

Principal PM Manager
Microsoft Corporation
@AnnaBarh



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA® Conference, RSA Security LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Security LLC or its affiliates. All rights reserved. RSA Conference logo, RSA and other trademarks are trademarks of RSA Security LLC or its affiliates.

Token Theft: All the Hip Kids Are Doing It.

Now What Are We Going to Do About It?

A color photograph of an elderly man with a joyful expression, standing outdoors at a fair or carnival. He is wearing a bright yellow polo shirt, a purple baseball cap, and dark trousers. In his left hand, he holds a large, fluffy pink cotton candy on a stick. In his right arm, he cradles a large, soft pink and purple stuffed animal, possibly a bear or elephant, which has several green and blue tickets attached to its front. The background is filled with the vibrant colors and decorations of a fairground, including a Ferris wheel and various booths. The overall atmosphere is one of fun and nostalgia.

#RSAC

#RSAC



A medium shot of a man and a woman at a carnival. The man, wearing a straw hat, sunglasses, a white button-down shirt with red stripes on the suspenders, and blue jeans, is leaning over a metal railing, handing a red ticket stub to the woman. He has a mustache and is smiling. The woman, with blonde hair pulled back, is wearing a yellow t-shirt under a denim vest, a yellow wristband, and a small star-shaped earring. She is also smiling. In the background, a large Ferris wheel with red and white gondolas is visible against a blue sky with scattered white clouds. The number '15' is printed on the side of one of the gondolas. The overall atmosphere is festive and suggests a fun day at the fair.

#RSAC

TICKETS



Welcome To
WONDER WHEEL

Since 1920
Wonder Wheel No height requirement
Speek-a-Rama No height requirement
Thunderball Must be at least 48" tall
Bumper Cars Must be at least 48" tall
Scrambler Must be at least 48" tall

*Tickets purchased here are for
Densey's Wonder Wheel Park ONLY
*Please check height requirements
and restrictions for certain rides
*Absolutely NO REFUNDS

Thank you and Have Fun!

SPECIAL
5 Tickets \$30.00

Credit
Card
Accepted

TICKETS

WONDER

WHEEL

PARK

A promotional image featuring a smiling man with blue eyes and a wide white smile. He is wearing a vibrant red uniform consisting of a tall, cylindrical hat with a dark band and a matching zip-up jacket. The jacket is adorned with a decorative border of shiny gold sequins. He is also wearing white gloves. In his right hand, he holds up a bright yellow rectangular card with the words "SEASON PASS" printed on it in black capital letters. The background is a dark, atmospheric setting with several bright, multi-colored stage lights (red, orange, yellow) creating starburst effects and lens flare. The overall mood is festive and celebratory.

#RSAC



#RSAC

County Fair SSO



Resource / Workload



Access Token



Refresh Token



Identity Provider



Client / Browser



Credentials



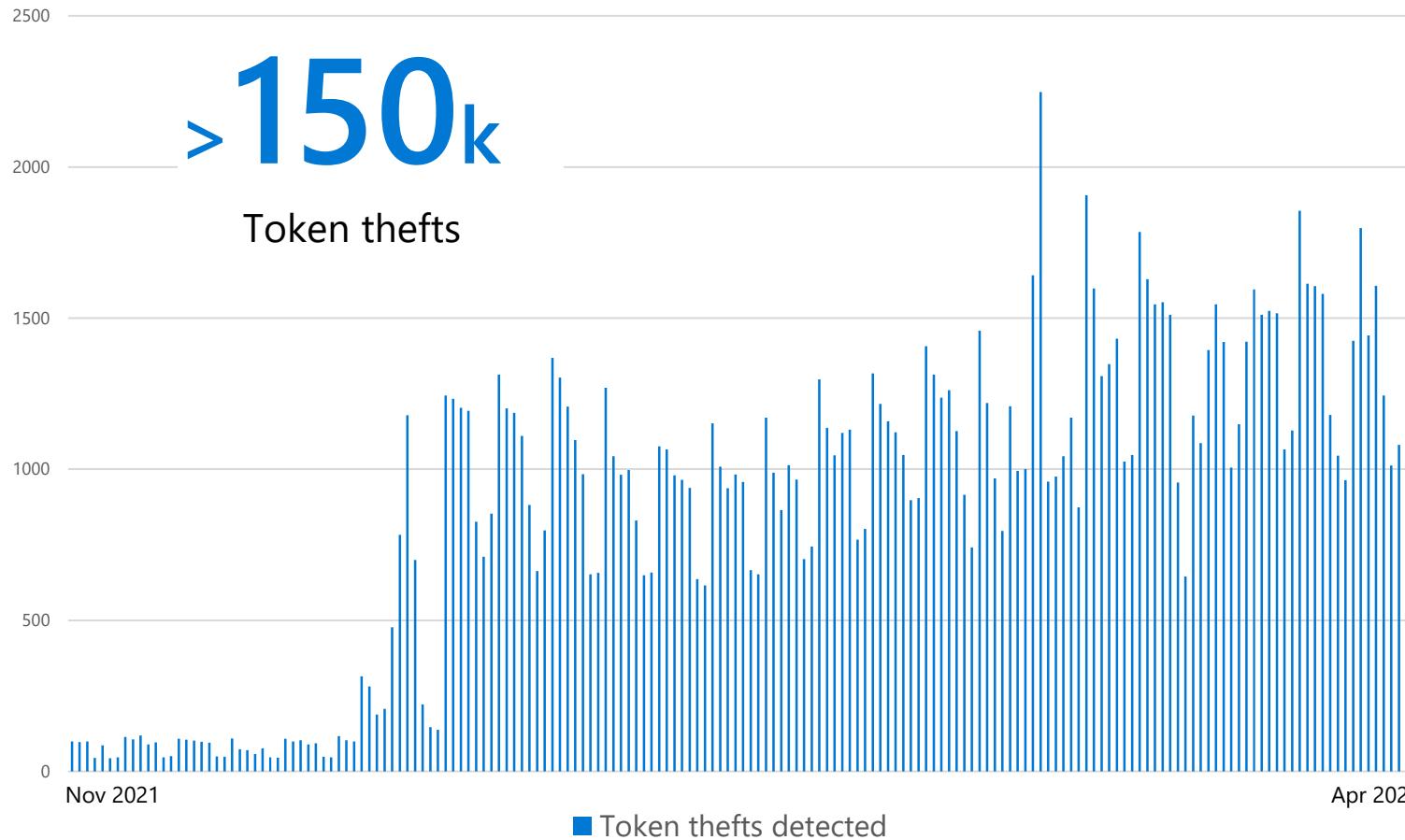
Token Theft: The Mugged Guest





#RSAC

Detected in the last six months:



>1.7M
Device malware infections





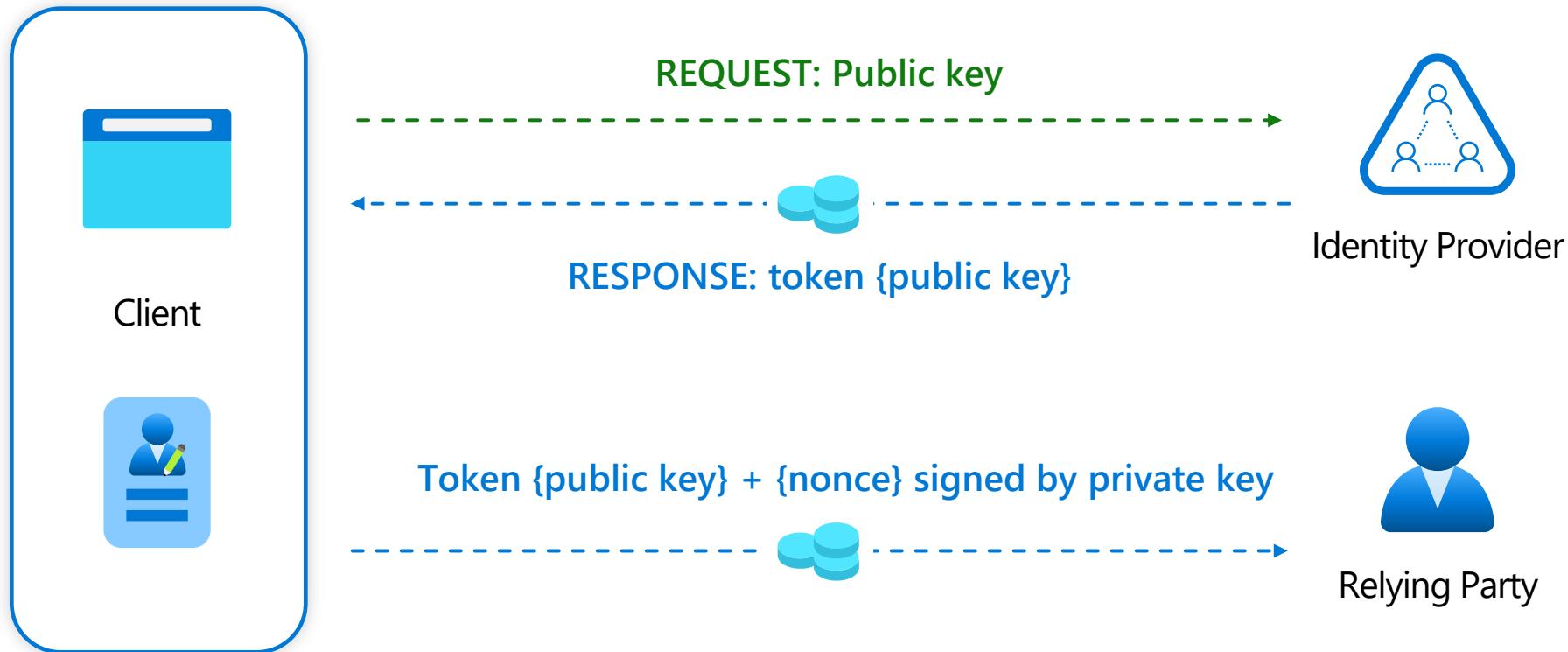
A woman in a red shirt is screaming with her mouth wide open. She is surrounded by several zombies with pale skin and dark hair. One zombie has its hands on her shoulders, another is behind her head with its mouth open, and a third is partially visible on the right. A hand is reaching out from a wooden door handle on the right side of the frame. The door has the letters "DPOP" written on it. The background is dark and appears to be an industrial or basement setting.

TLS Token
Binding

Signed
Header
Request

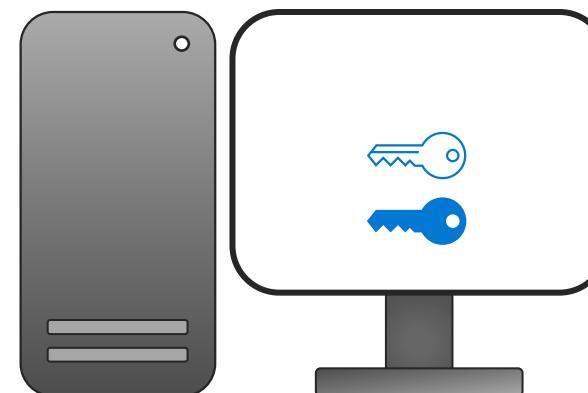
A Bit of History

It is a simple protocol!



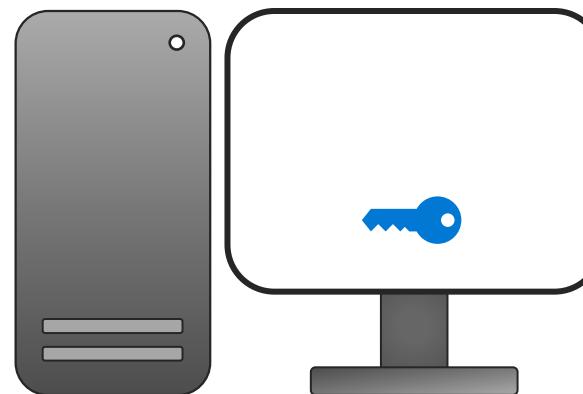
Let's try it...

We established
that it is a
simple protocol
– So let's
implement it!



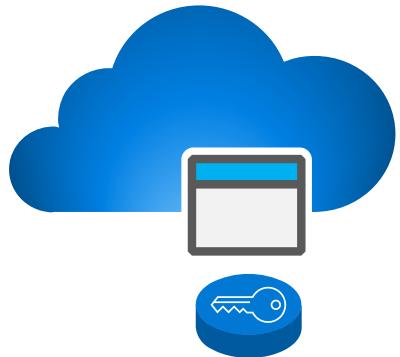
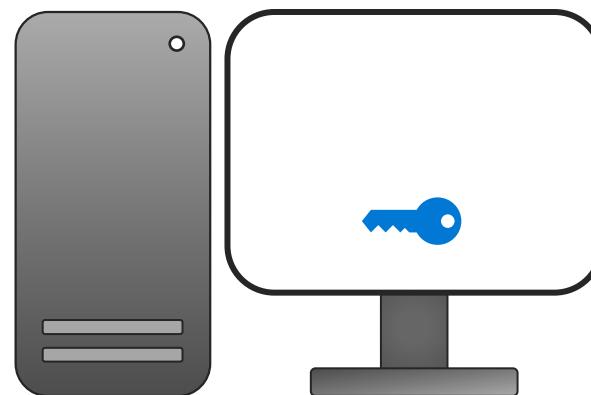
Let's try it...

We established
that it is a
simple protocol
– So let's
implement it!



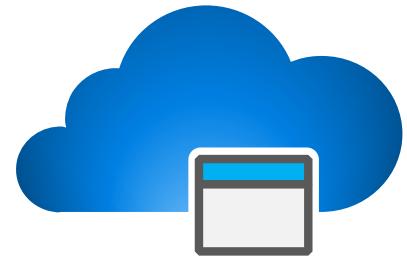
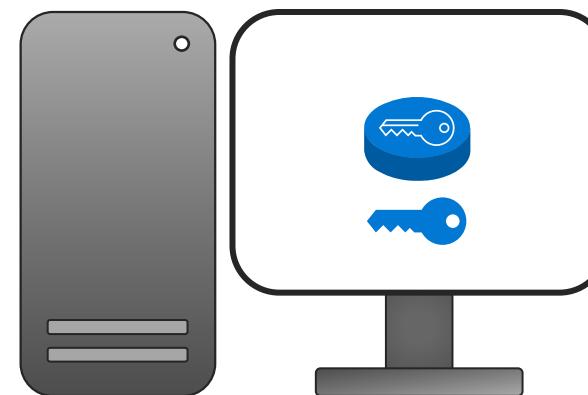
Let's try it...

We established
that it is a
simple protocol
– So let's
implement it!

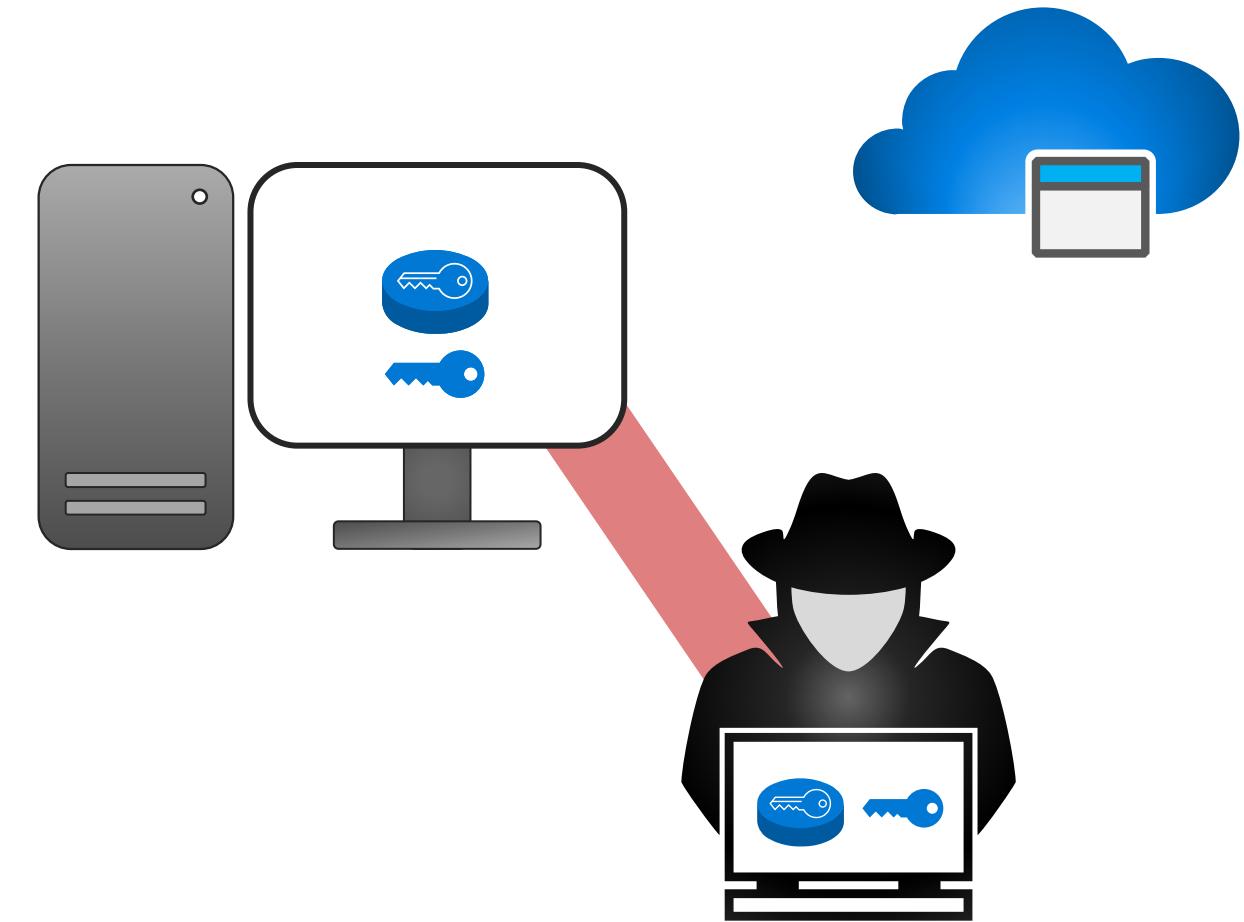


Let's try it...

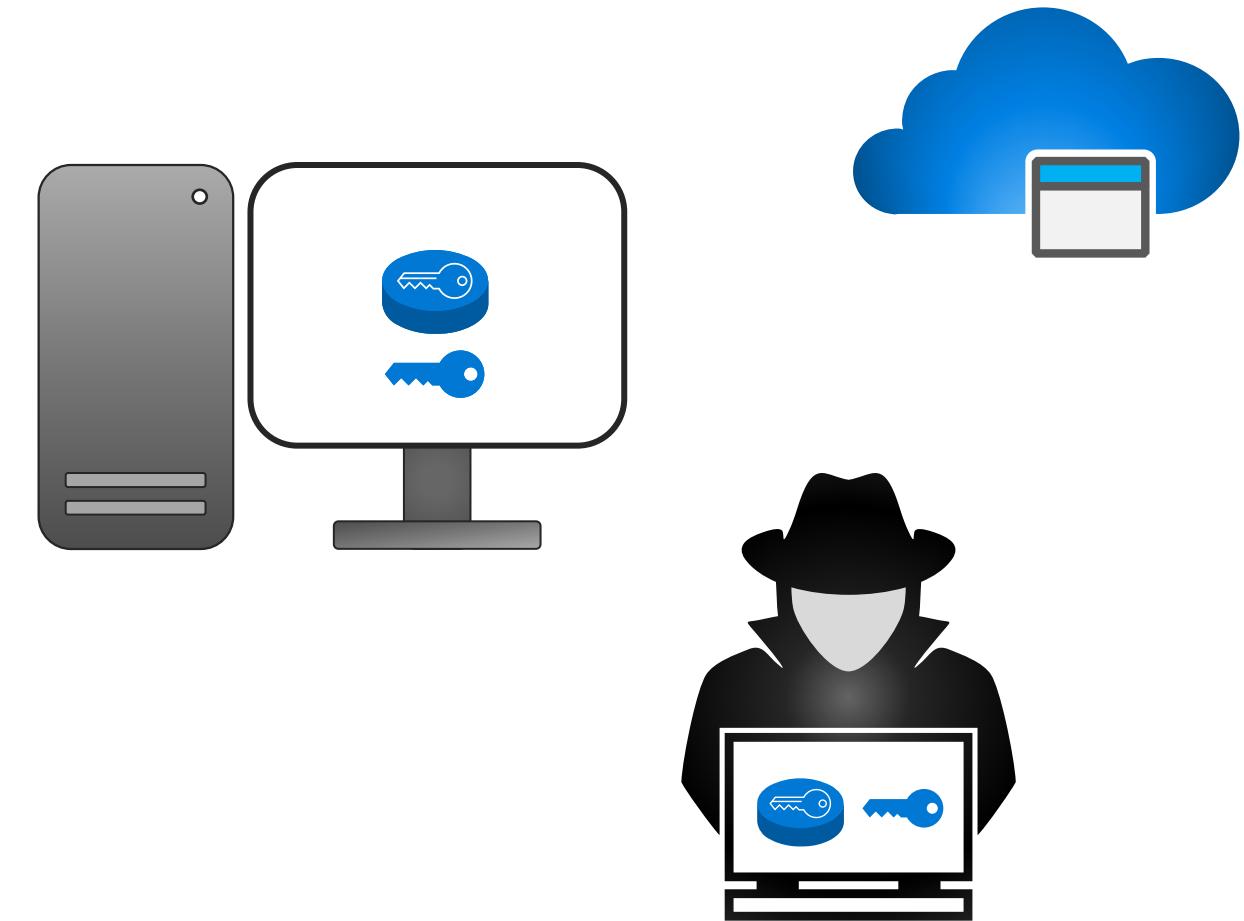
We established
that it is a
simple protocol
– So let's
implement it!



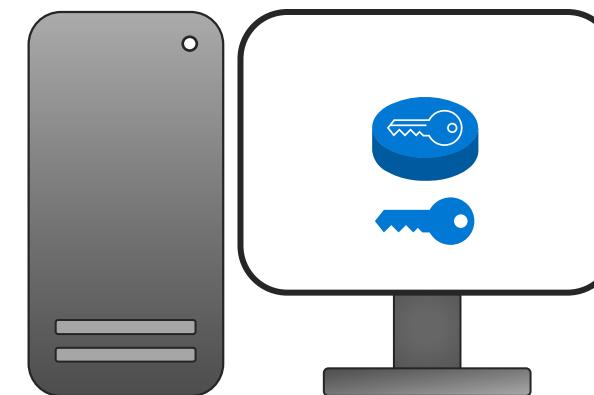
Oh, but there is a problem . . .



Oh, but there is a problem . . .

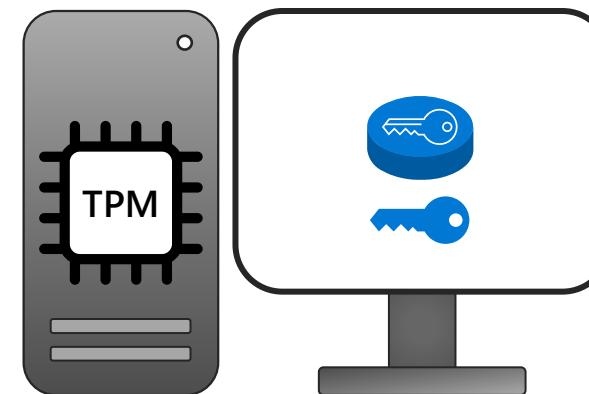


We can solve it



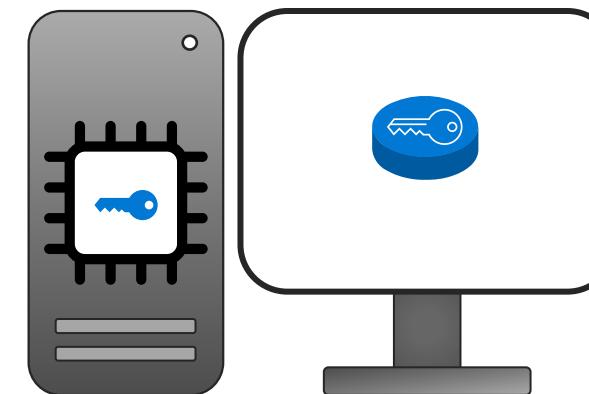
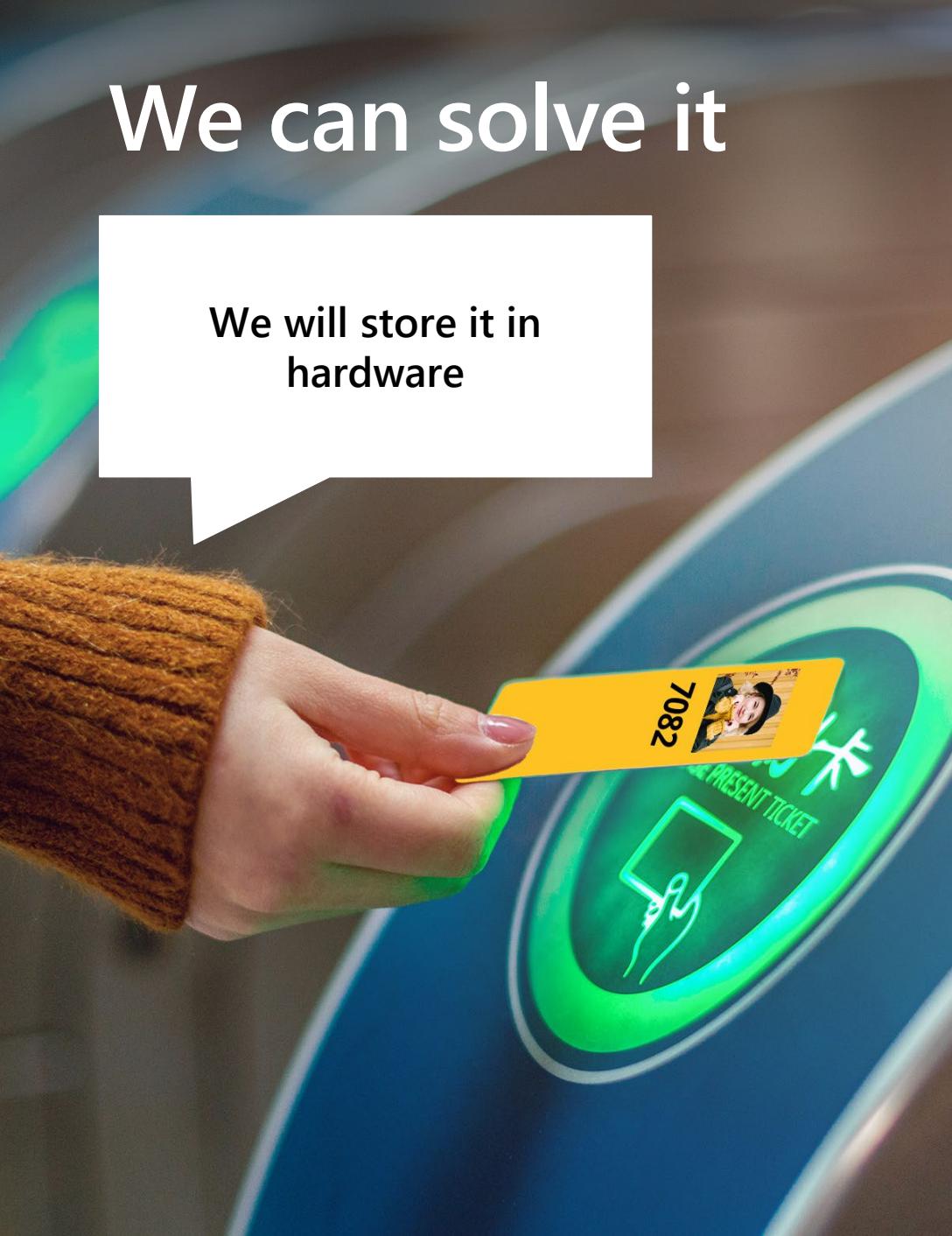
We can solve it

We will store it in hardware



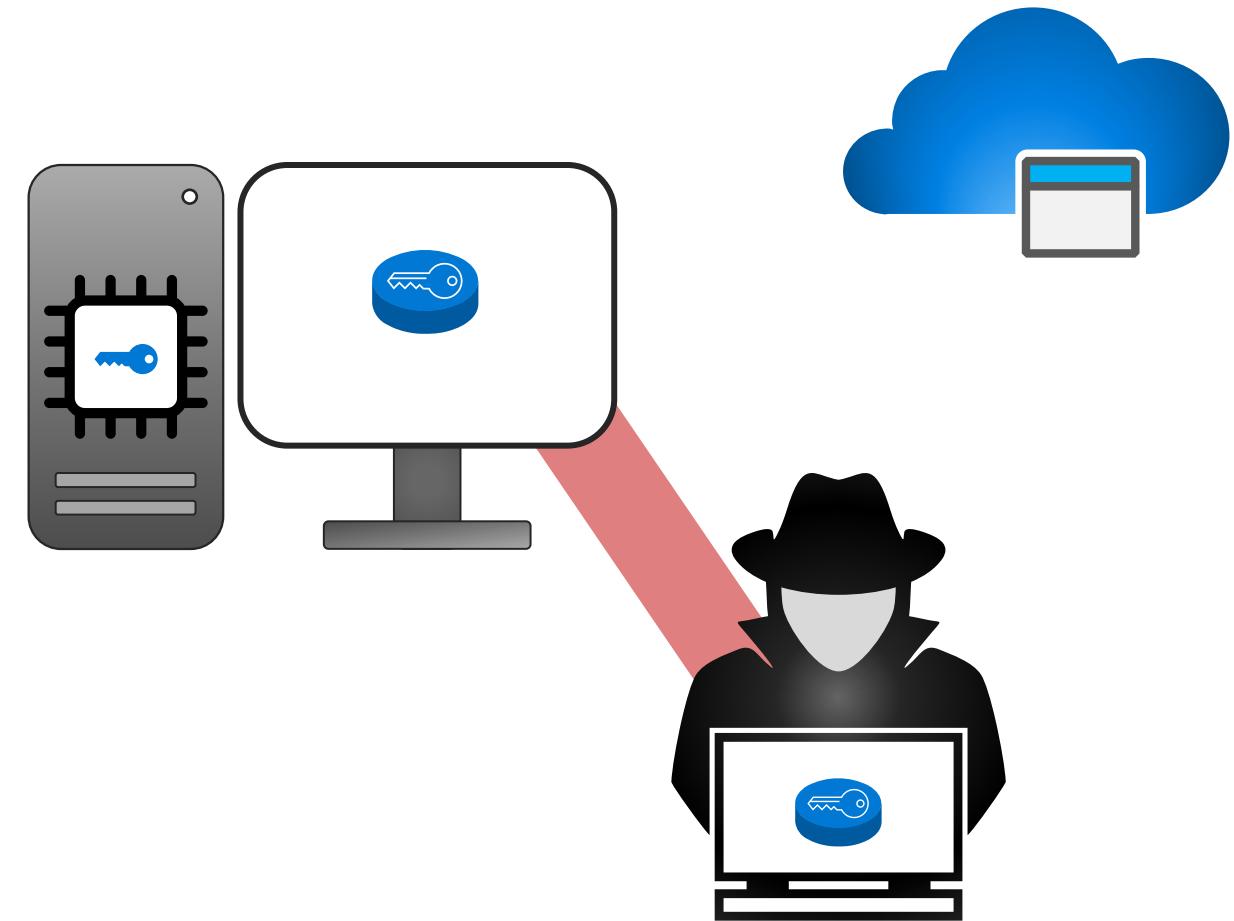
We can solve it

We will store it in hardware



We can solve it

We will store it in hardware



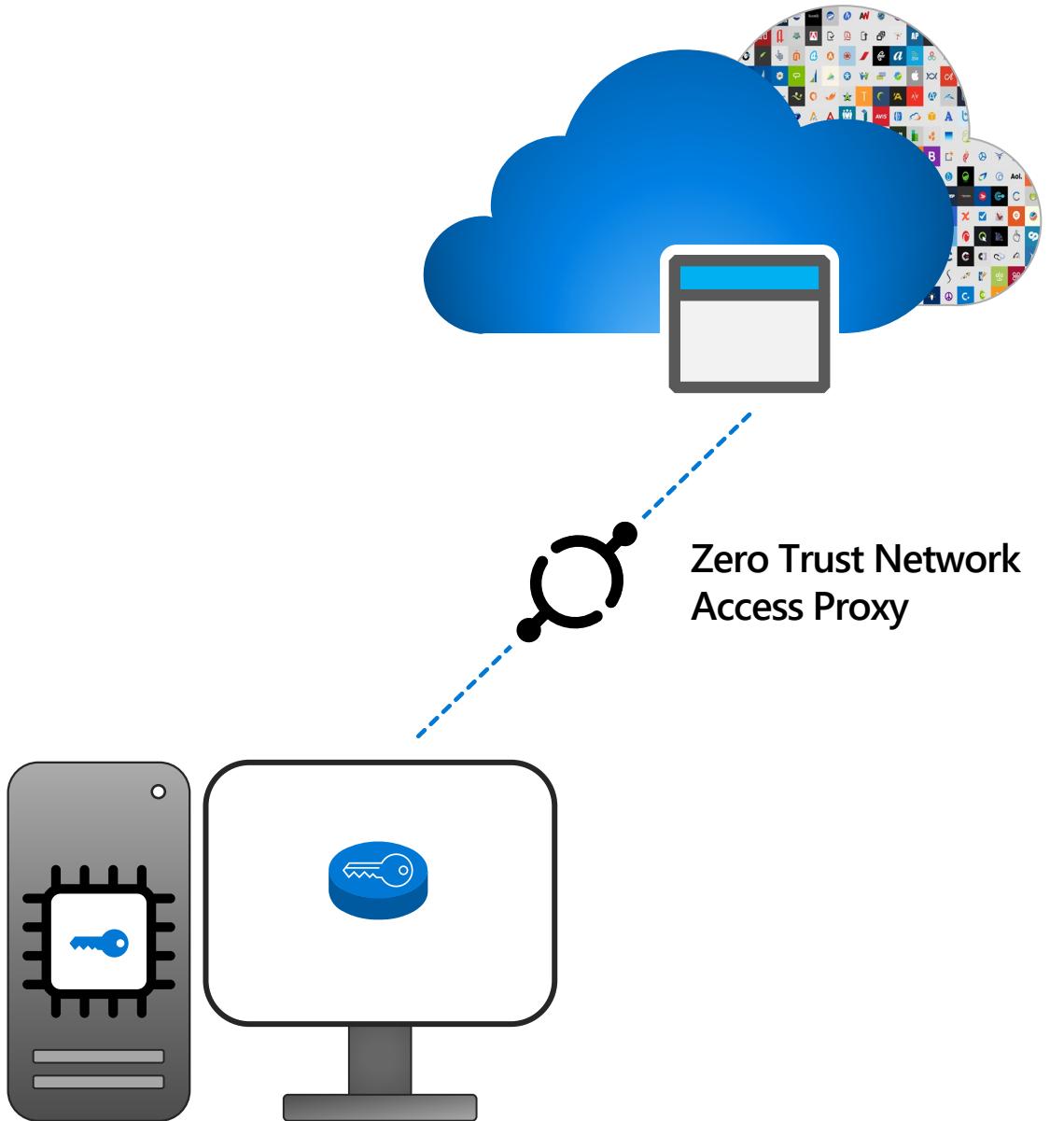
The problem with your face

The problem with your face

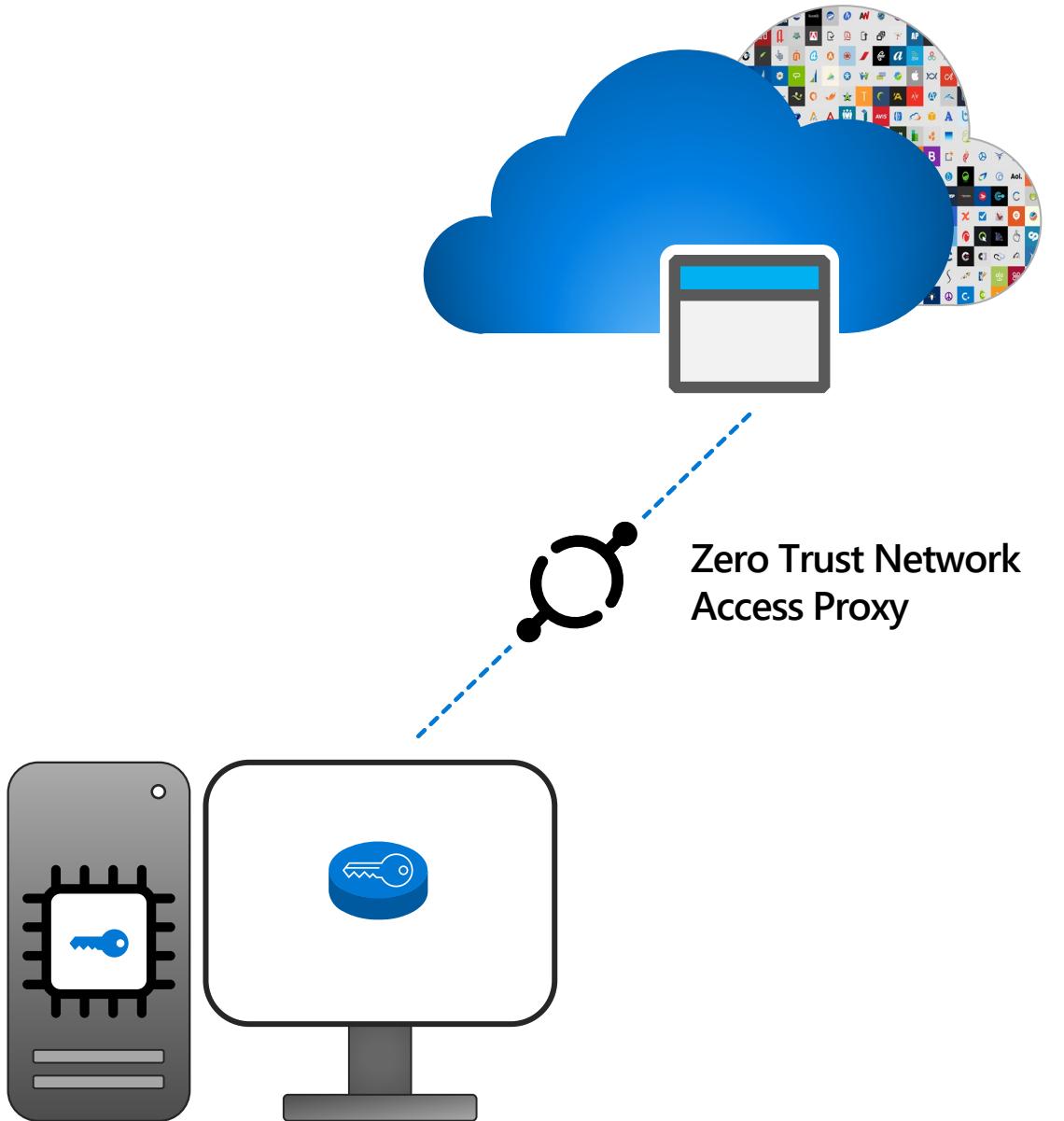


3.5M+
applications

Friendly wrappers

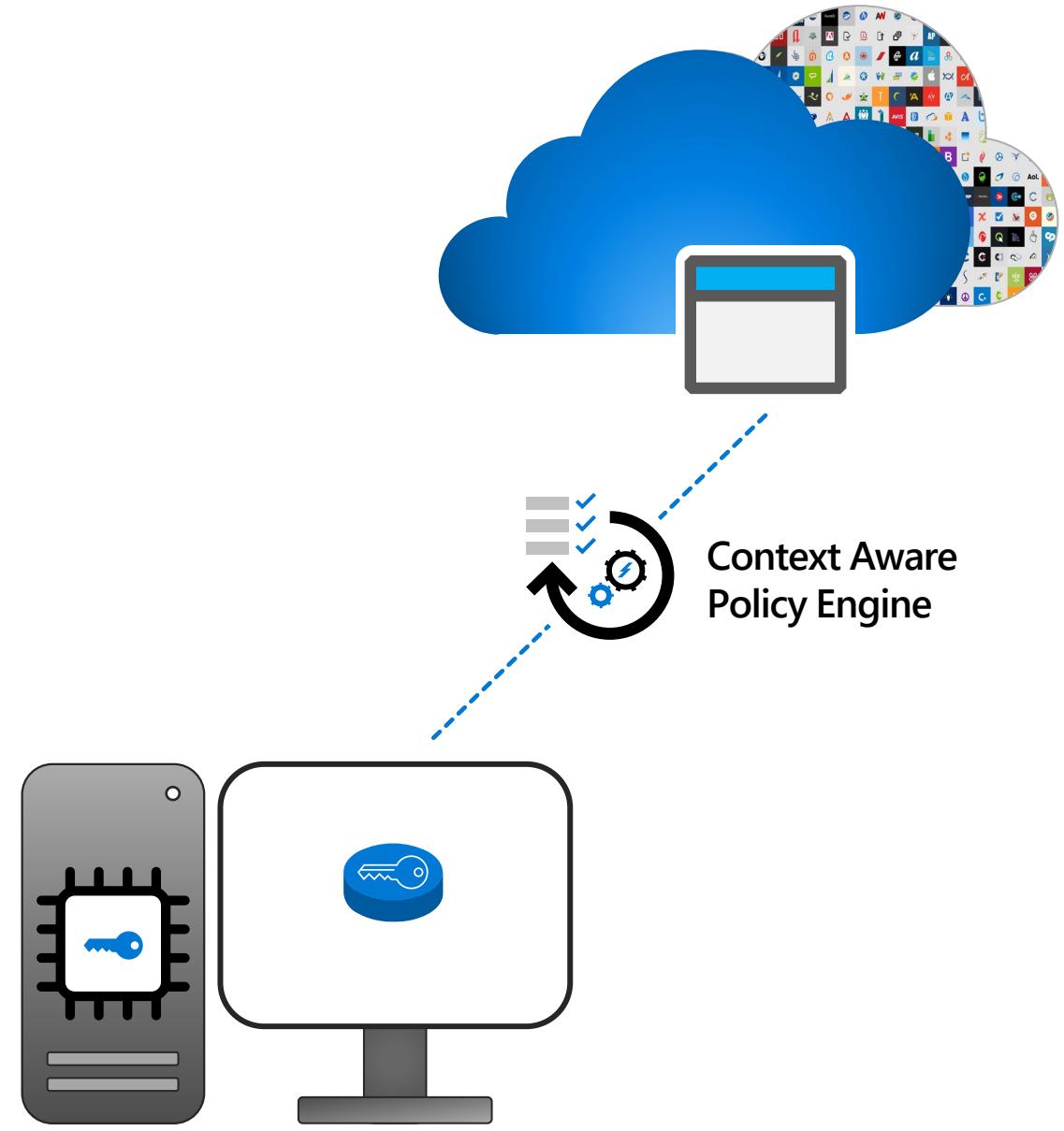
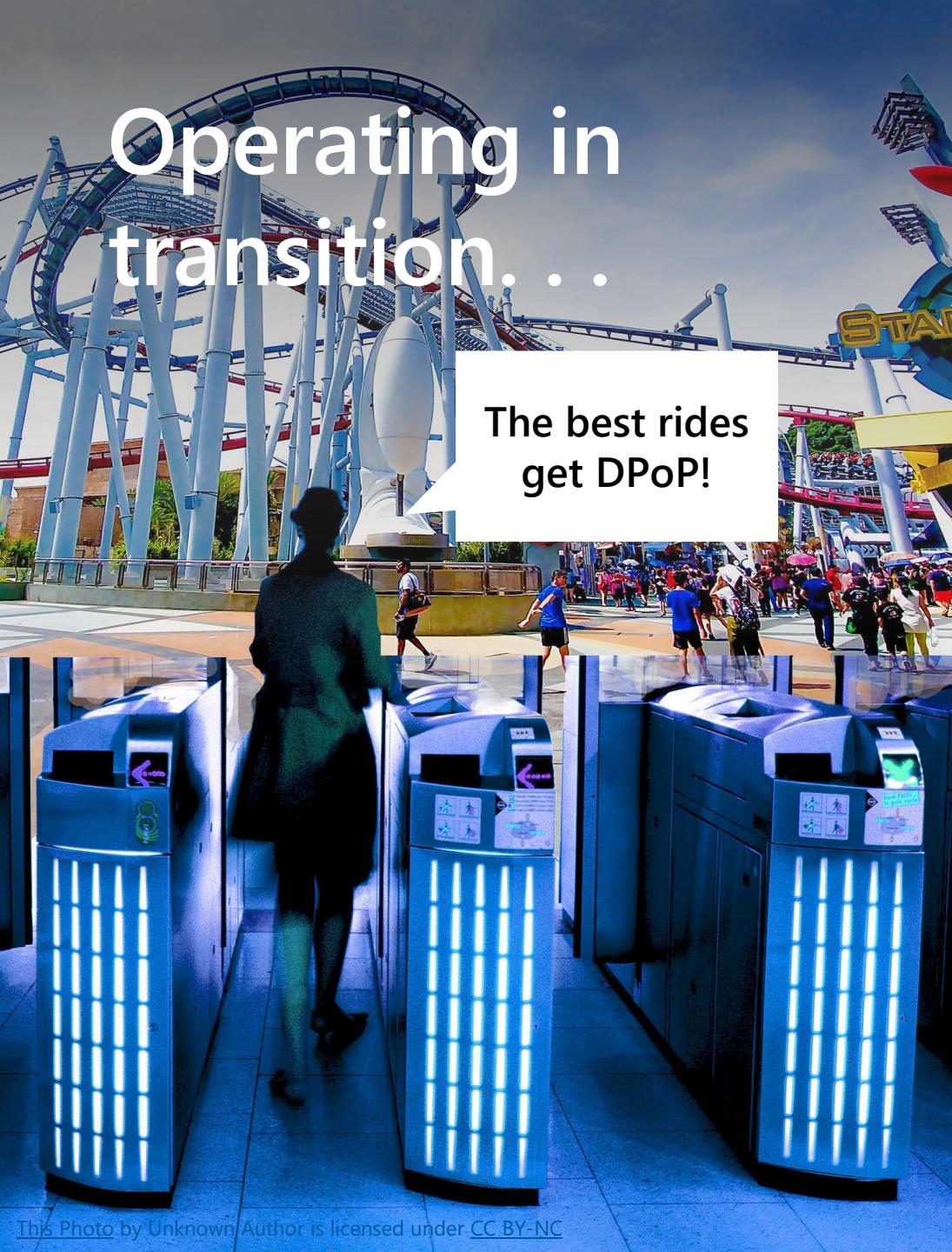


Friendly wrappers



Operating in transition. . .

The best rides
get DPoP!



Resident Malware

Resident malware can piggyback on legitimate requests – but DPoP forces malware to stay active (making it much more detectable).



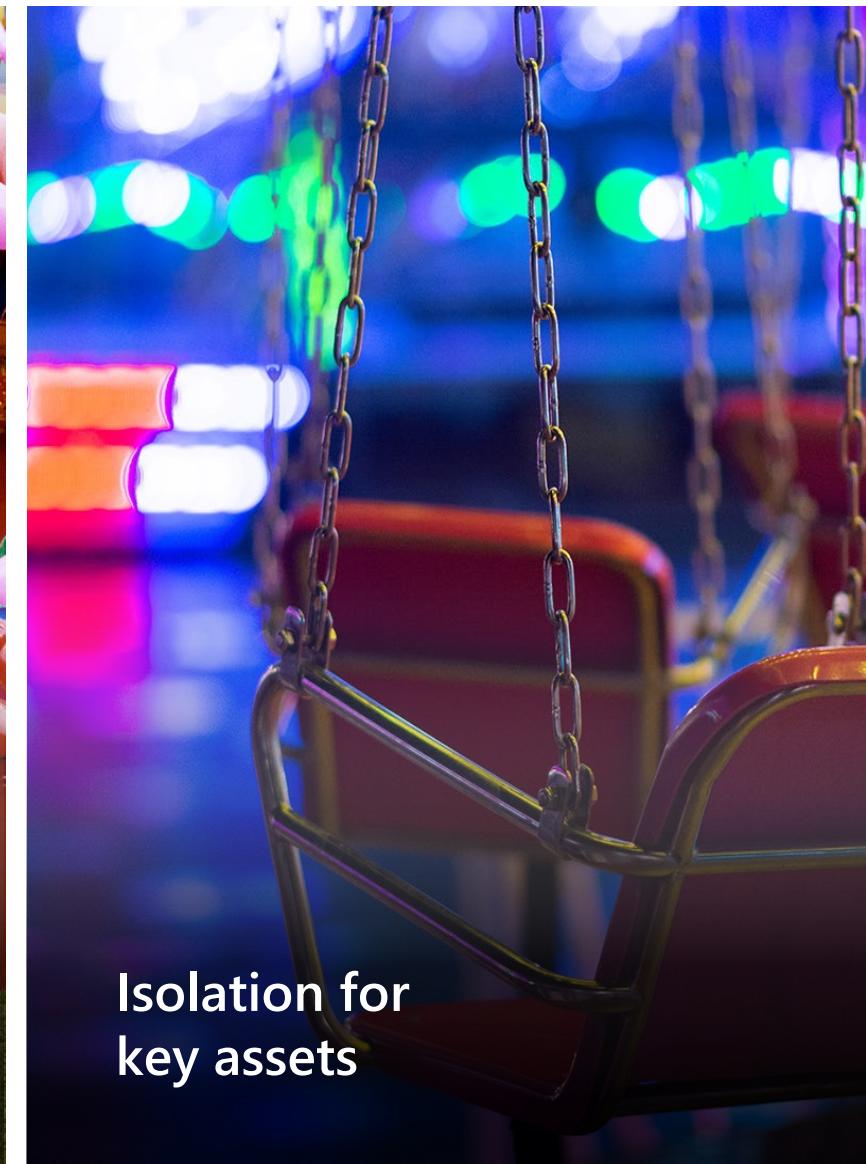
What do we do in the meantime?



Detections



Endpoint protection



Isolation for key assets

DPoP is the
solution for
token theft



Thank you

**Alex Weinert**

Director of Identity Security
Microsoft Corporation
@Alex_T_Weinert

**Anna Barhudarian**

Principal PM Manager
Microsoft Corporation
@AnnaBarh

