

CISCO TRUSTED ROOT STORE

CABF MEETING 46



TRUST

don't worry, this is gonna work out just fine

VERY DEMOTIVATIONAL .com

ADDING TRUST BITS

- ▶ Tech changes to add trust bits to P7Bs in progress
- ▶ Will definitely want at least Server TLS, Code Signing, Device Identity
- ▶ Current multi-file approach needs to stick around
 - ▶ Supports devices with earlier non-bit releases
 - ▶ Provide multiple sizes for smaller memory footprint requirements

ios.p7b
"Original Recipe"



ios_union.p7b
"Extra Crispy"



ios_core.p7b
"Grilled Lite"



codesign.p7b
"Mashed Potatoes"



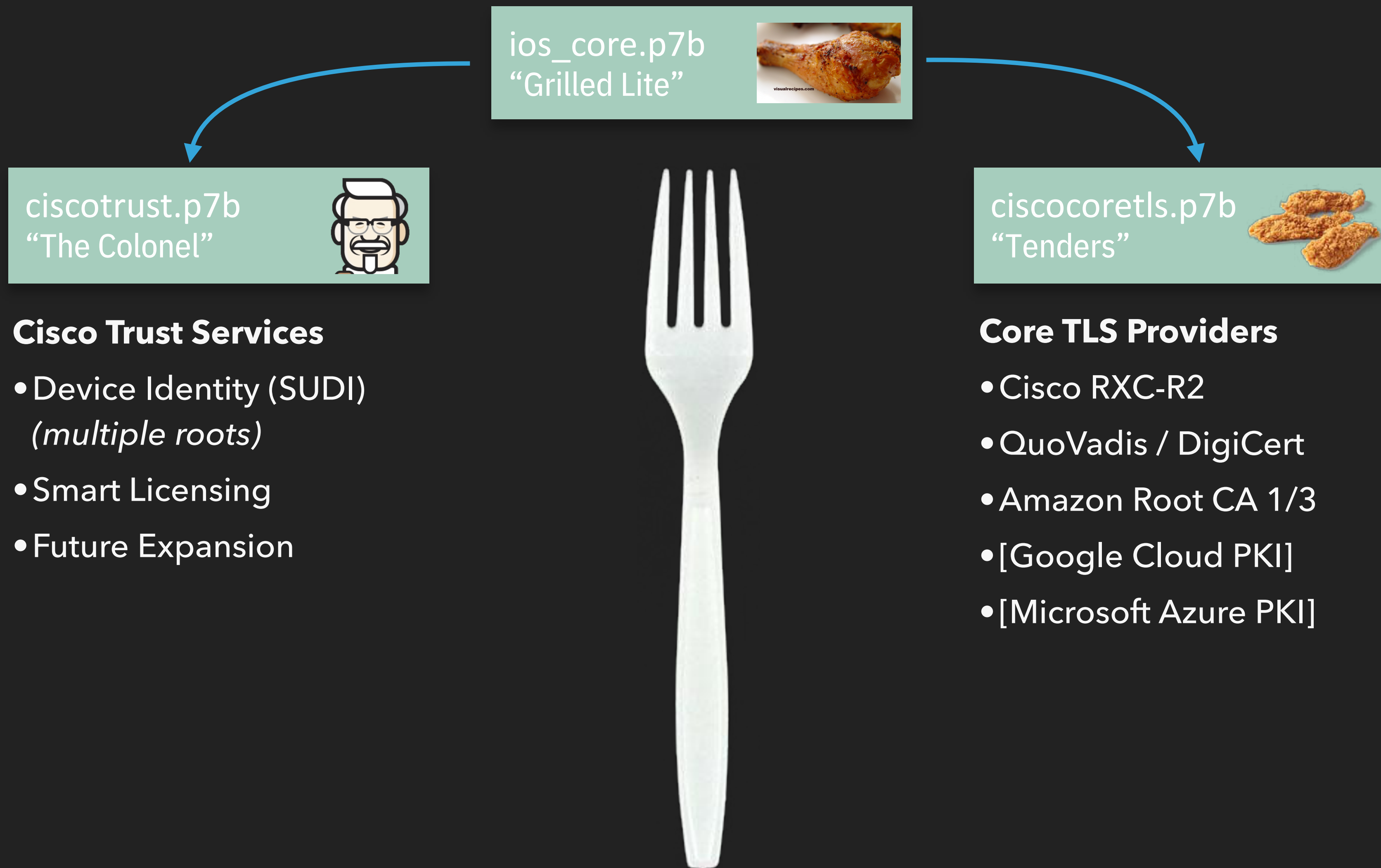
device.p7b
"Mac & Cheese"



CORE BUNDLE NEEDS TO SPLIT

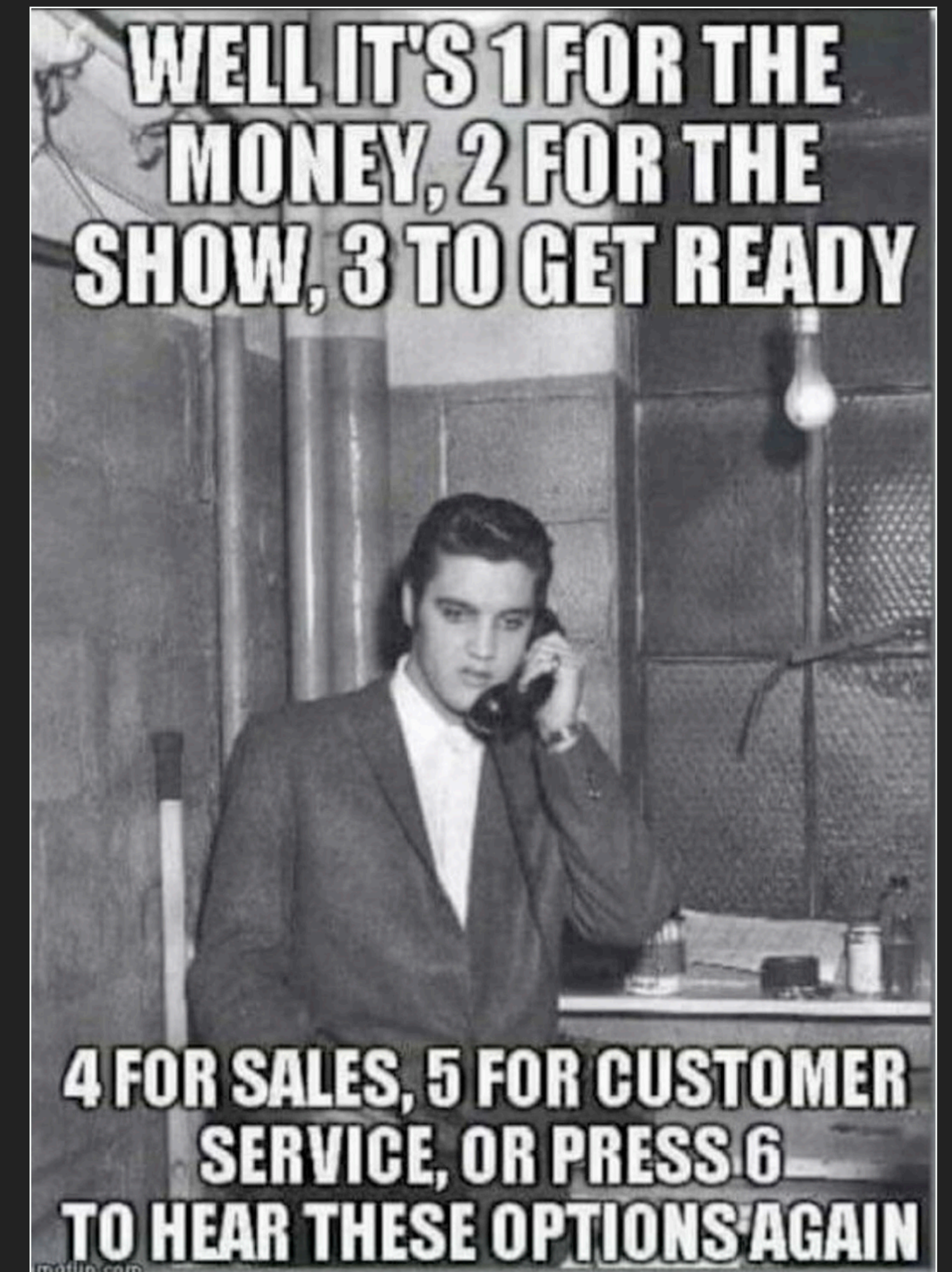
- ▶ We want separation of Cisco-specific private functions like licensing from mutable stores like TLS.
 - ▶ We can then encourage devs to keep the immutable set in protected memory
- ▶ With the expansion of our Core TLS CA set, the split will help out devices with smaller memory footprints

STICKING A FORK IN THE CORE



DIVING INTO THE CCADB

- ▶ We've been happy to (finally!) move more fully into the CCADB
- ▶ In the next year:
 - ▶ Replace the contents of Intersect with validations from CCADB
 - ▶ Open a formal inclusion request process through CCADB



I HAVE
NO IDEA

WHAT'S GOING ON
SO HERE'S A PICTURE
OF A DINOSAUR IN A TOP HAT
AND MONOCLE, RIDING ON
A SEGWAY



QUESTIONS?