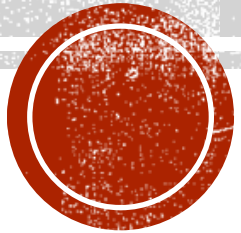
DARK-WEB DEMYSTIFIED

Feel the Power of Anonymity!



29th September, 2018

Adarsh Nair, CISSP

UST Global®
Innovation • Information • Technology

Profile

Name	**:**	**Adarsh S V Nair**
Designation	**:**	**Project Manager & Sr. Security Analyst**
Organization	**:**	**UST Global Inc.**
Certifications	**:**	**CISSP, OSCP, ISO LA, LPT, ECSA, CHFI, CEH**
Honorary Positions	**:**	**Deputy Commander - Kerala Police Cyberdome** **Advisory Board Member, EC-Council USA** **Board Member, OWASP Kerala**
Qualification	**:**	**M.Tech (Information Security), B.Tech (CSE)**
Publications	**:**	**2 (IEEE and ACM)**

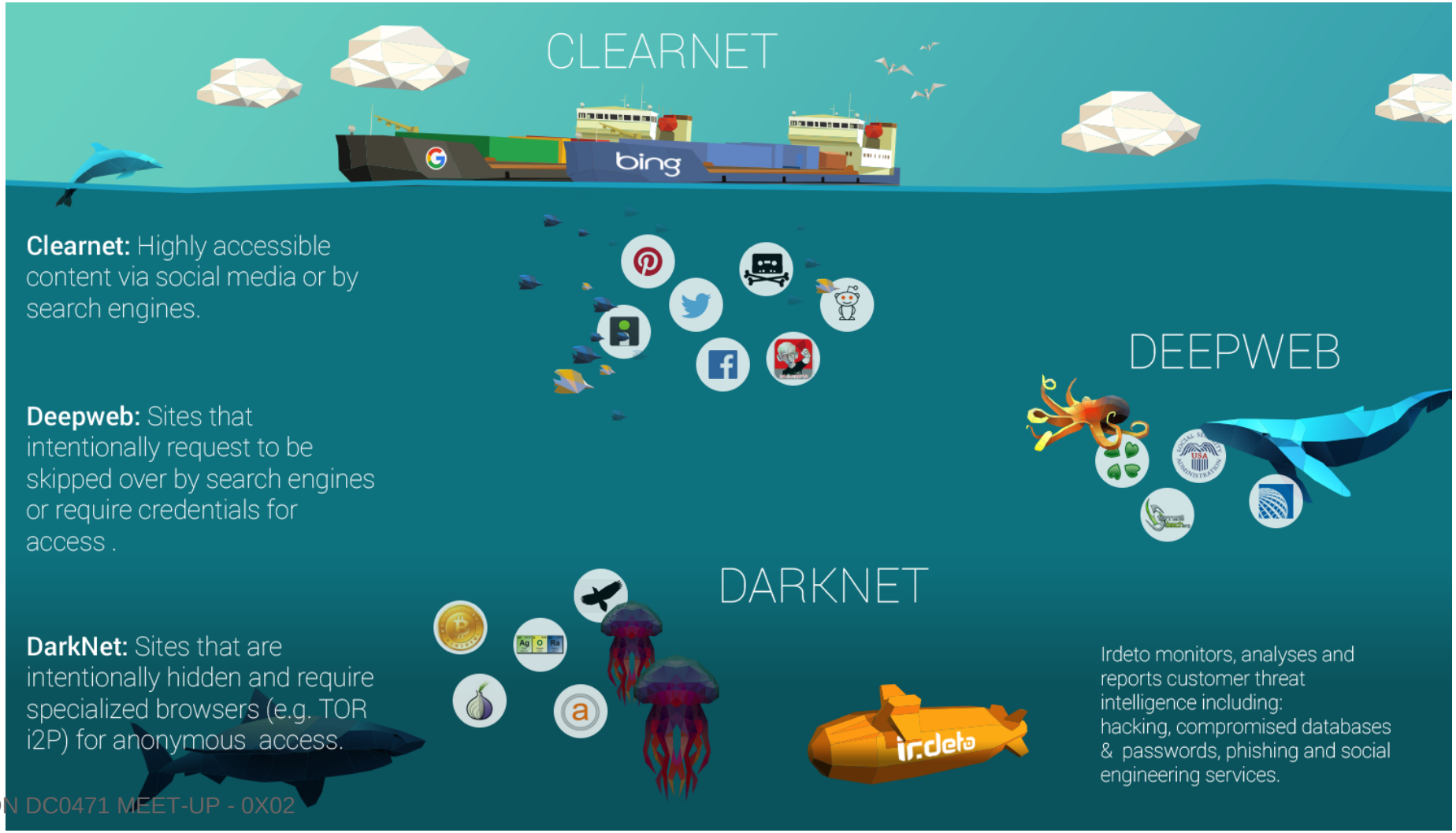
AGENDA

- Introduction
- Types of Web
- Dark Web
- Onion Routing
- ToR – The Onion Router
- ToR – Anonymity
- ToR – Onion Services
- Conclusion
- References

INTRODUCTION

- Dark Web is where you can operate without being tracked, maintaining total anonymity.
- These are hidden networks avoiding their presence on the Surface Web, and its URLs are tailed up with **.onion**.
- ToR is a distributed overlay network which anonymizes TCP-based applications (e.g. web browsing, secure shell, instant messaging applications.)
- Dark Web sites are hosted as ToR onion services.
- Commonly used for illegal businesses.
- With the help of ToR, the web users can roam around the Internet without any fear, keeping themselves and their real identities hidden from law enforcement agencies.

TYPES OF WEB


CLEARNET
bing
Clearnet: Highly accessible content via social media or by search engines.
Deepweb: Sites that intentionally request to be skipped over by search engines or require credentials for access .
DEEPWEB
DarkNet: Sites that are intentionally hidden and require specialized browsers (e.g. TOR i2P) for anonymous access.
DARKNET
Irdeto monitors, analyses and reports customer threat intelligence including: hacking, compromised databases & passwords, phishing and social engineering services.

DARK WEB

- The **dark web** (or dark net) is a small part of the deep web.
- No tracking, maintaining total anonymity.
- Contents are not accessible through search engines.
- It is the anonymous Internet.
- Within the dark net, both web surfers and website publishers are entirely anonymous.
- The Dark Web is much smaller than the Deep Web and is made up of all different kinds of websites that sell drugs, weapons and even hire assassins.
- **[websitename].onion** domains are not indexed by regular search engines, so you can only access Dark Web with special software.

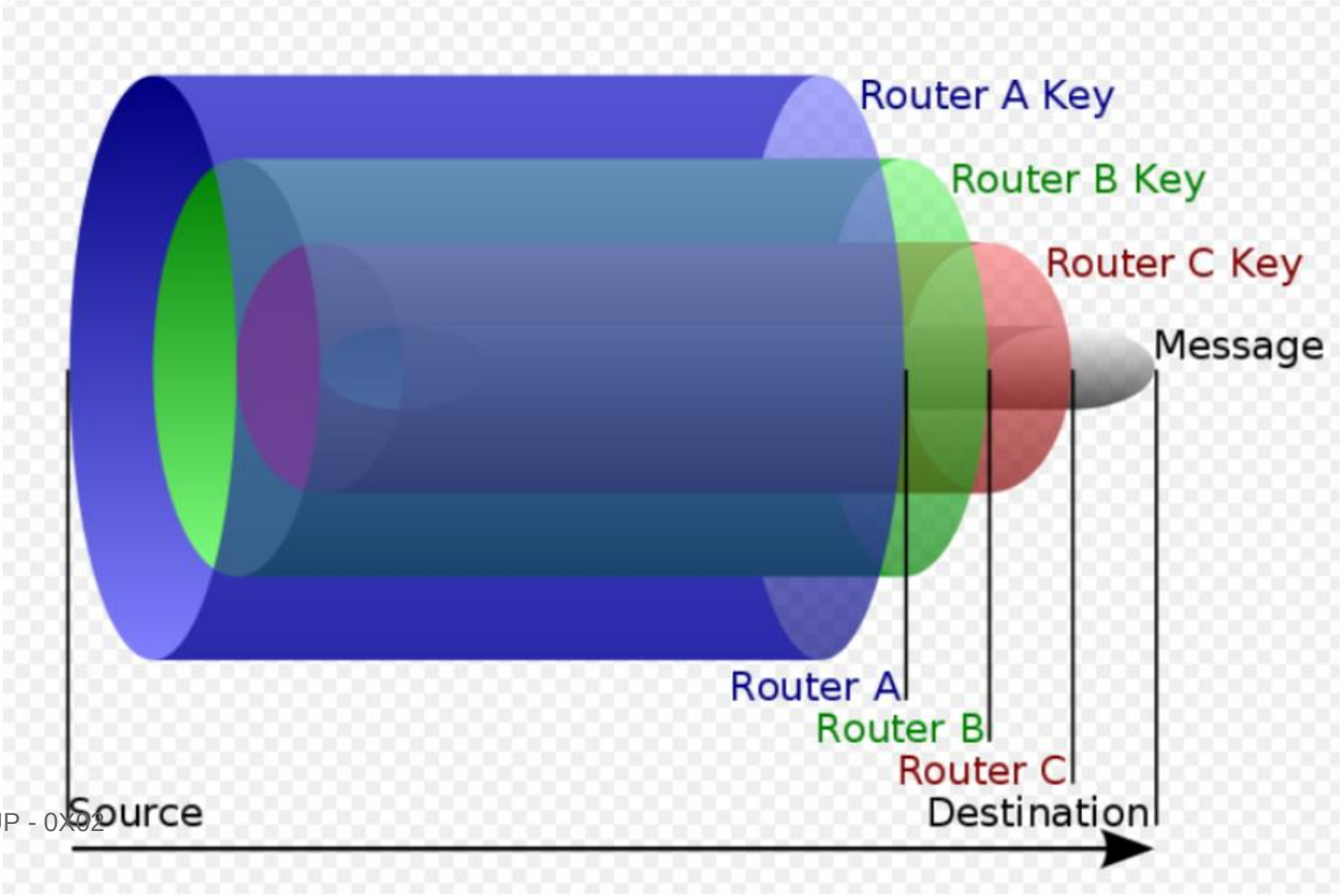
ONION ROUTING (OR)

- Onion routing is an anonymous communication technique over a computer network.
- Messages are constantly encrypted and then sent through several network nodes called onion routers which creates a circuit of nodes.
- Messages are put in cells and unwrapped at each node or onion router with a symmetric key.
- Each onion router removes a layer of encryption with its symmetric key to reveal routing instructions, and sends the message to the next router where this process is repeated.
- The ORs only know the successor or predecessor but not any other Onion Router.
- This prevents these intermediary nodes from knowing the origin, destination, and contents of the message.

TOR - THE ONION ROUTER

- Protect your privacy. Defend yourself against network surveillance and traffic analysis.
- For enabling anonymous communication.
- ToR prevents people from learning your location or browsing habits.
- ToR directs Internet traffic through a free, worldwide, volunteer network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.
- It is more difficult for Internet activity to be traced back to the user: this includes visits to Web sites, online posts, instant messages, and other communication forms.
- Onion routing is implemented by encryption in the application layer of a communication protocol stack, nested like the layers of an onion.

TOR - THE ONION ROUTER
(CONTD.)



TOR - HISTORY

- “Onion routing”, was developed in the mid-1990s.
- By United States Naval Research Laboratory employees, mathematician **Paul Syverson** and computer scientists **Michael G. Reed** and **David Goldschlag**.
- Protecting U.S. intelligence communications online.
- Onion routing was further developed by DARPA (*Defense Advanced Research Projects Agency*) in 1997.
- ToR was developed by **Syverson** and computer scientists **Roger Dingledine** and **Nick Mathewson**.
- Launched on 20 September 2002.
- In 2004, the Naval Research Laboratory released the code for ToR under a free license.

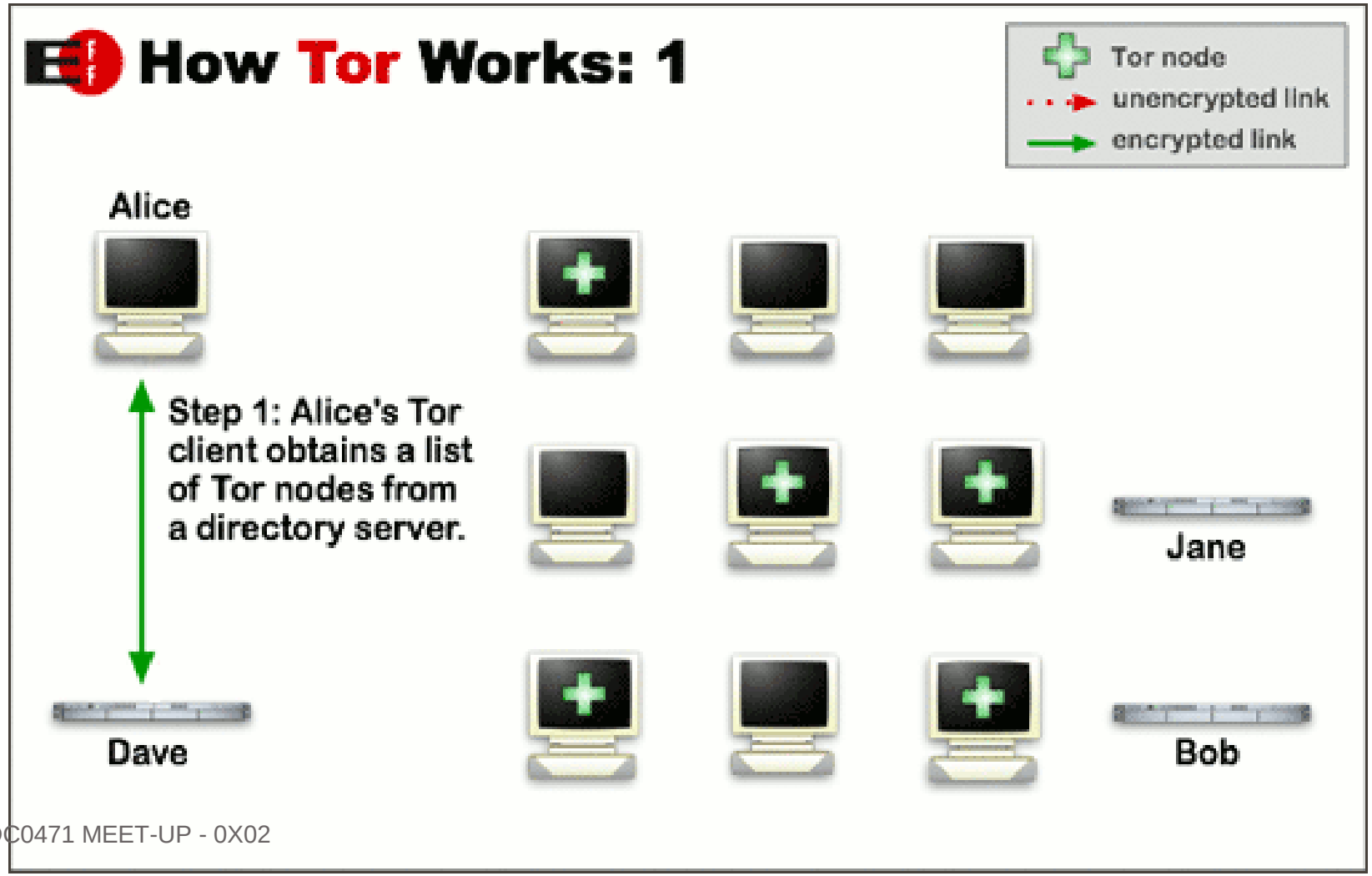
TOR - USERS

- Individuals also use ToR for socially sensitive communication: chat rooms and web forums for rape and abuse survivors, or people with illnesses.
- Journalists use ToR to communicate more safely with whistleblowers and dissidents.
- Non-governmental organizations (NGOs) use ToR to allow their workers to connect to their home website while they're in a foreign country, without notifying everybody nearby that they're working with that organization.
- Groups such as Indymedia recommend ToR for safeguarding their members' online privacy and security.
- Corporates use ToR as a safe way to conduct competitive analysis, and to protect sensitive procurement patterns from eavesdroppers.
- Law enforcement uses ToR for visiting or surveilling web sites without leaving government IP addresses in their web logs, and for security during sting operations.

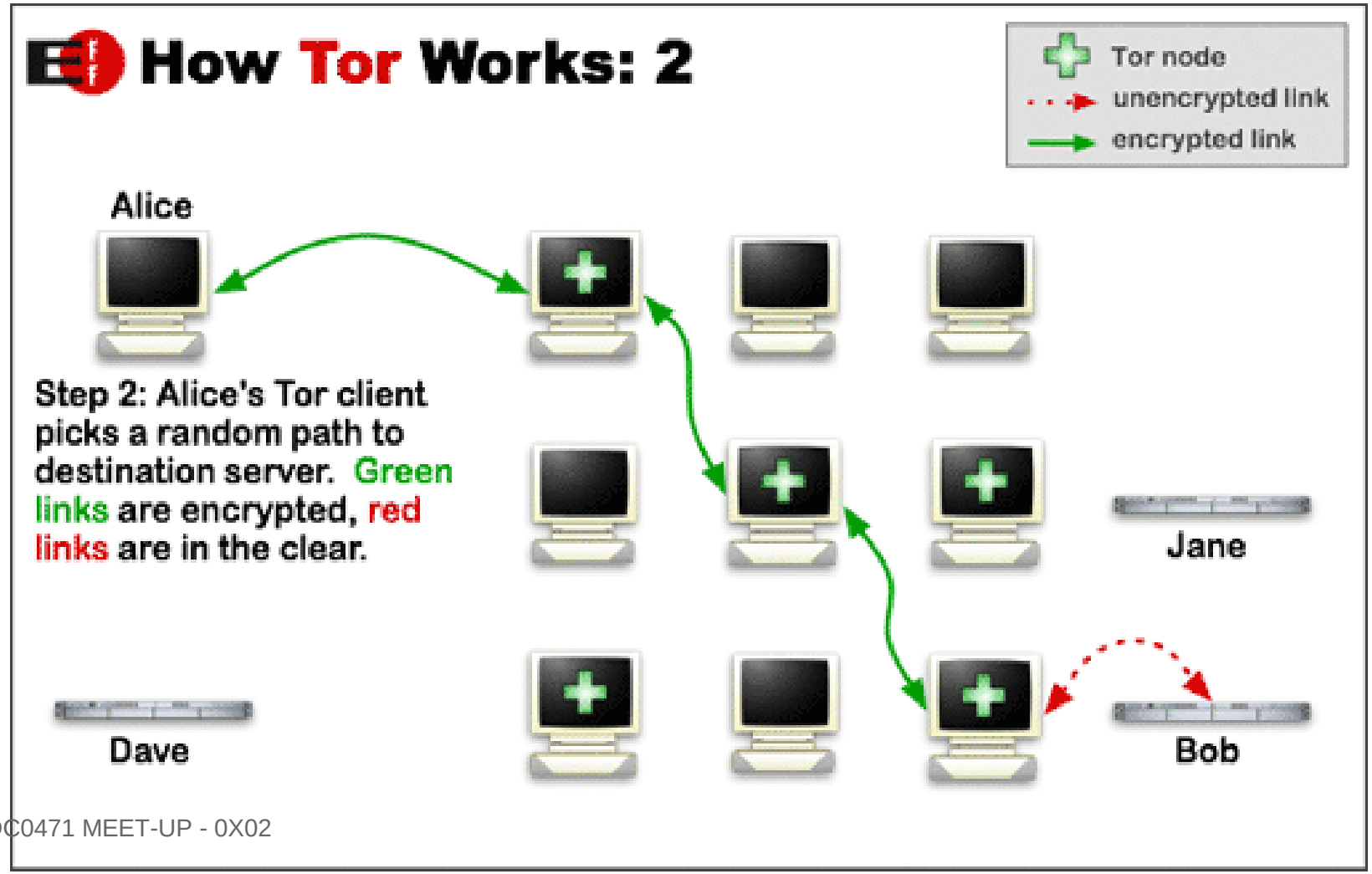
TOR - WORKING

- Data packets on the ToR network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going.
- The user's software or client incrementally builds a circuit of encrypted connections through relays on the network.
- The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to.
- No individual relay ever knows the complete path that a data packet has taken.
- For efficiency, the ToR software uses the same circuit for connections that happen within the same ten minutes.
- Later requests are given a new circuit, to keep people from linking your earlier actions to the new ones.

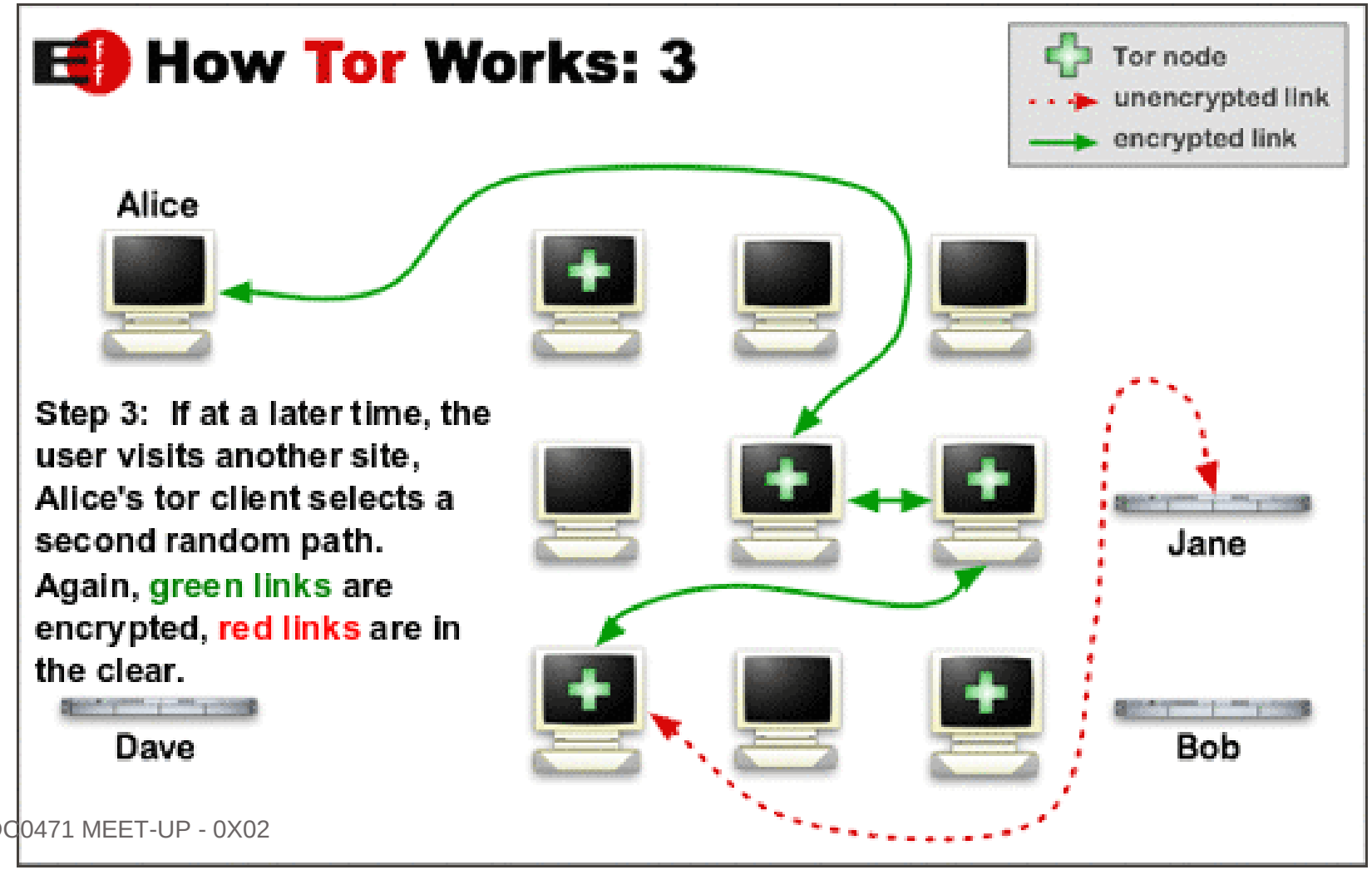
TOR - WORKING (CONTD.)



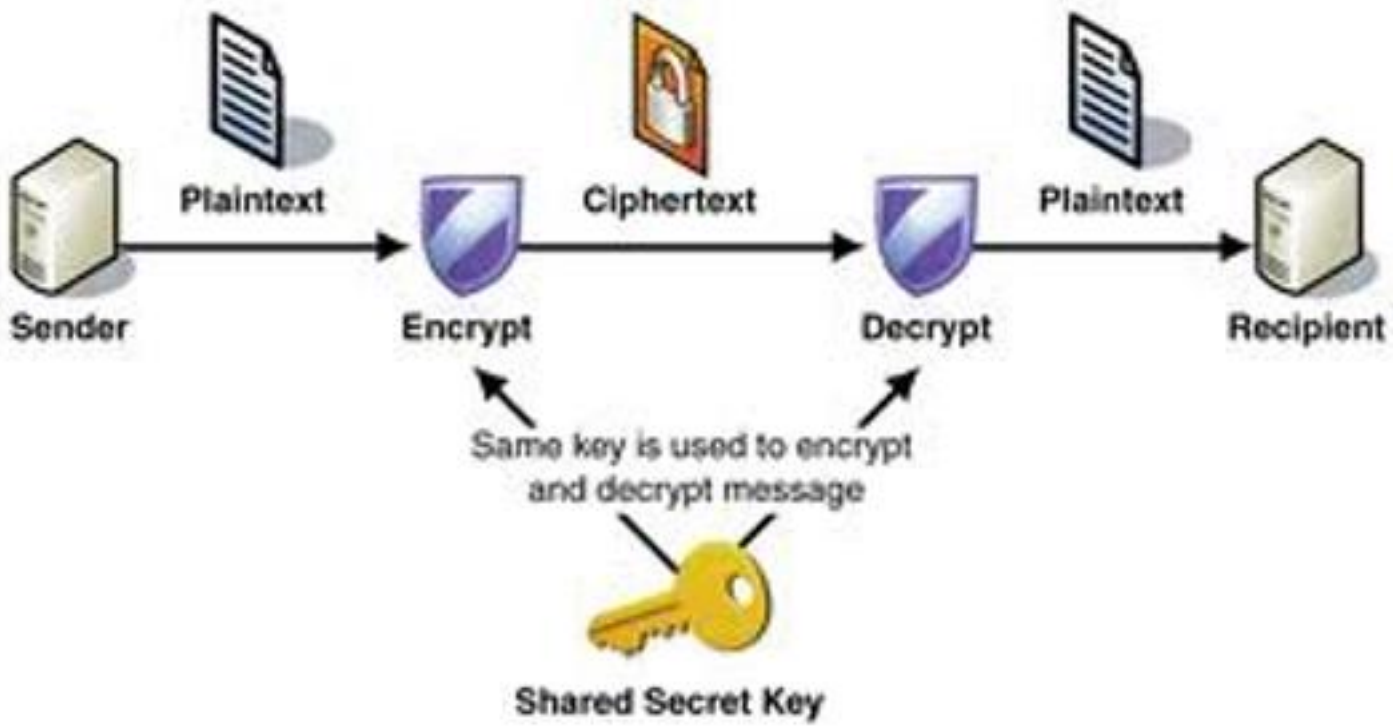
TOR - WORKING (CONTD.)



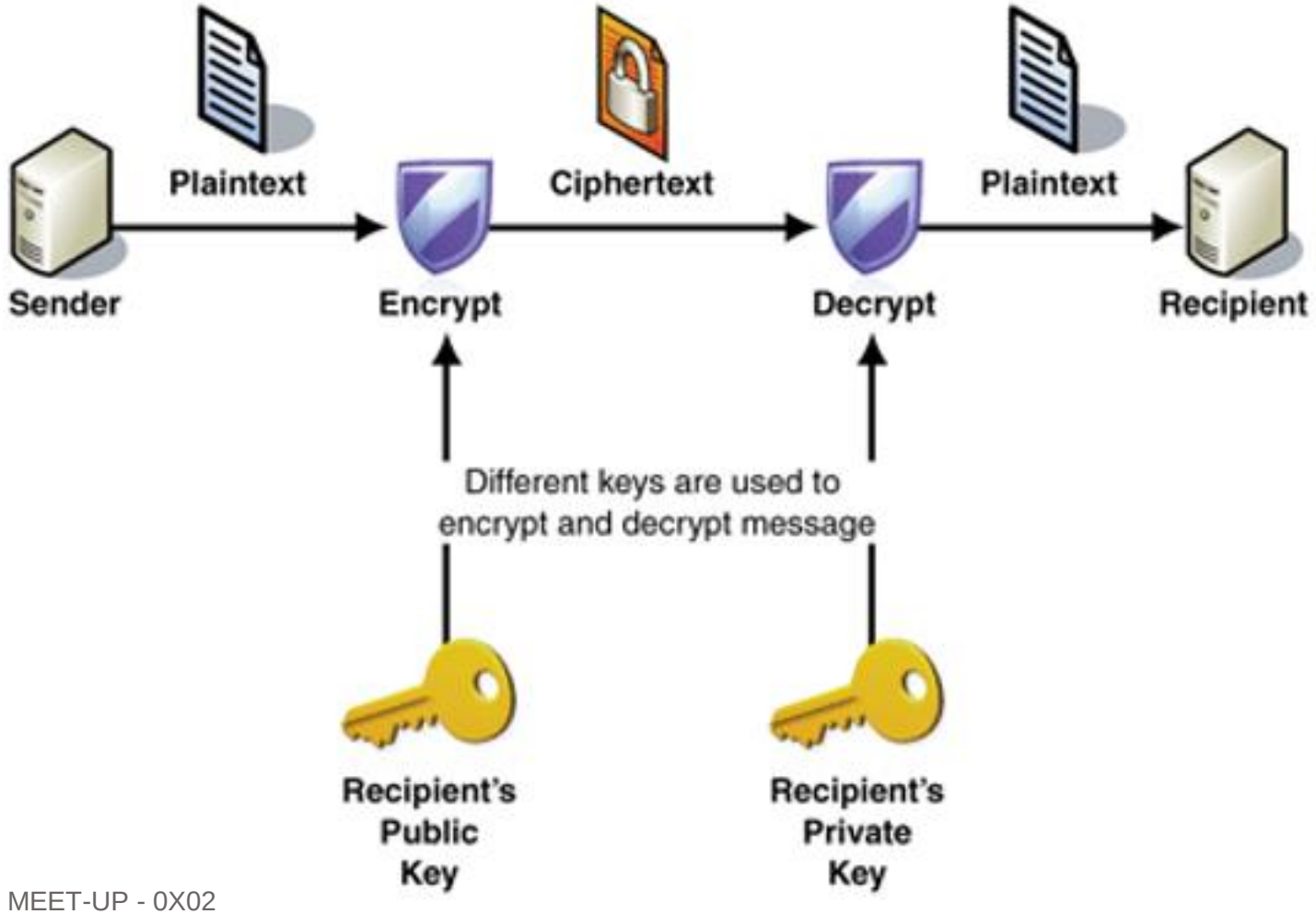
TOR - WORKING (CONTD.)



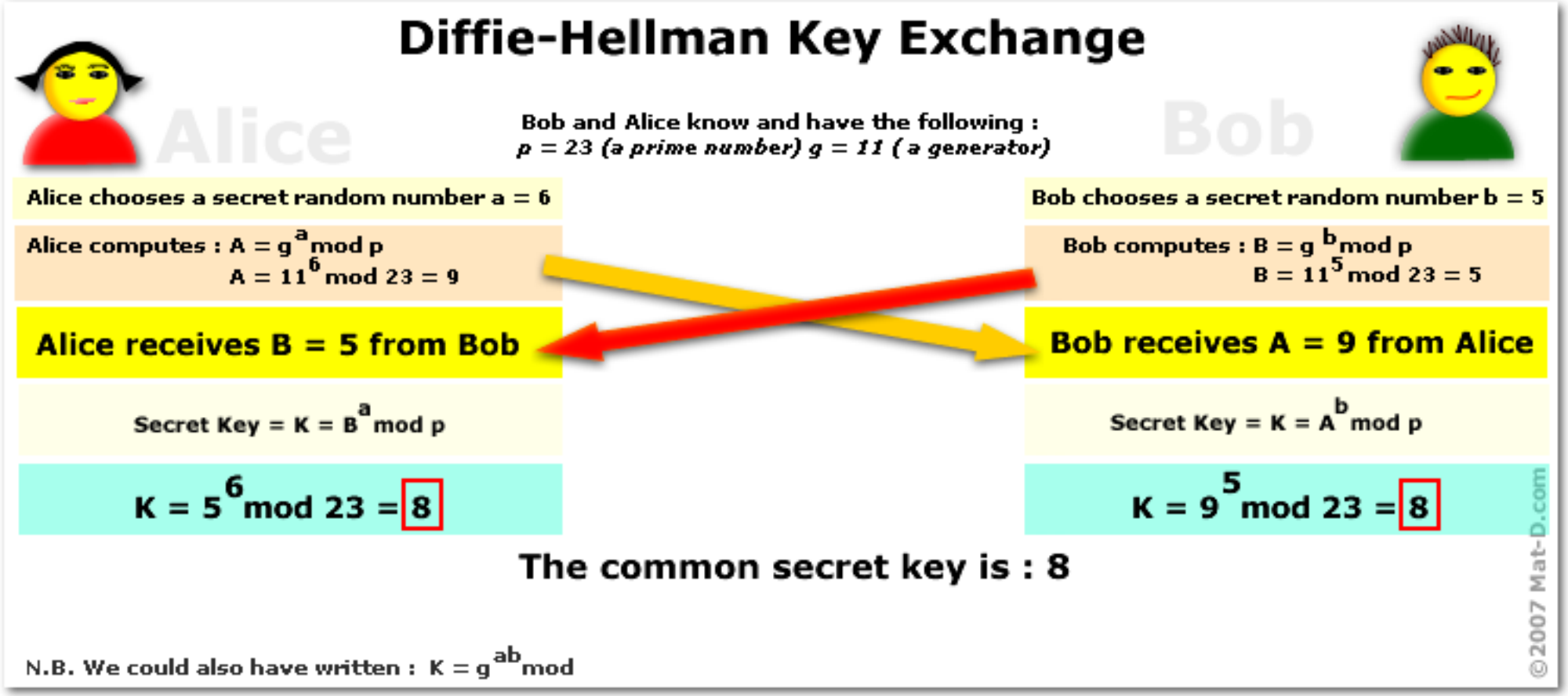
SYMMETRIC CRYPTOGRAPHY



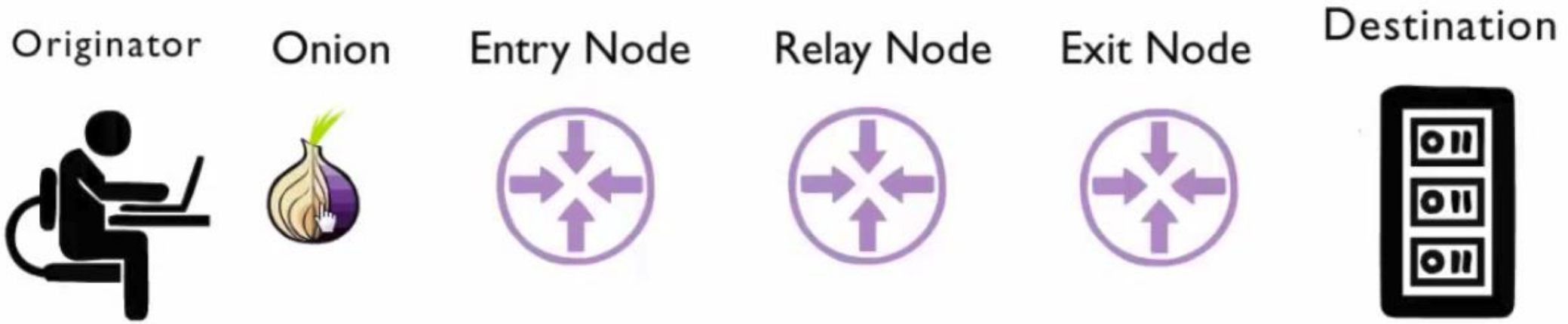
ASYMMETRIC CRYPTOGRAPHY



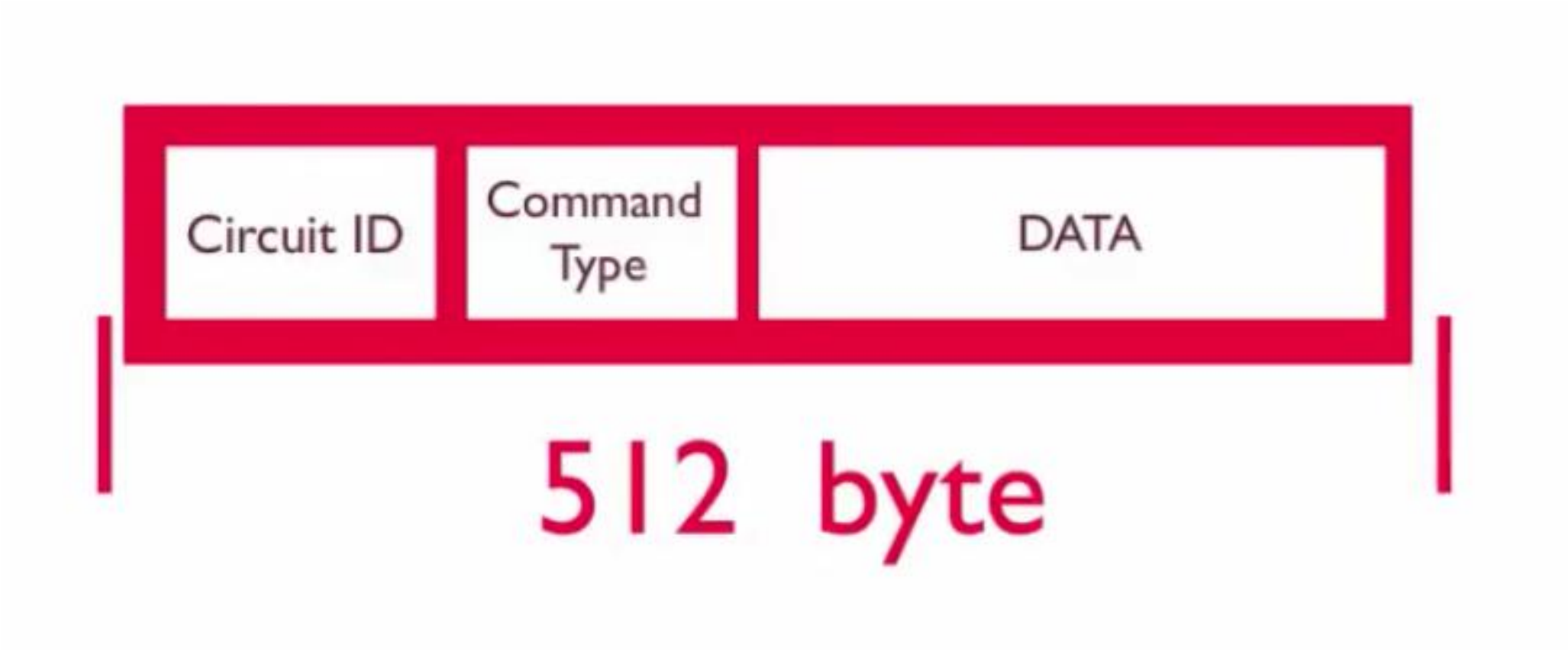
DIFFIE-HELLMAN KEY EXCHANGE



TOR - COMPONENTS



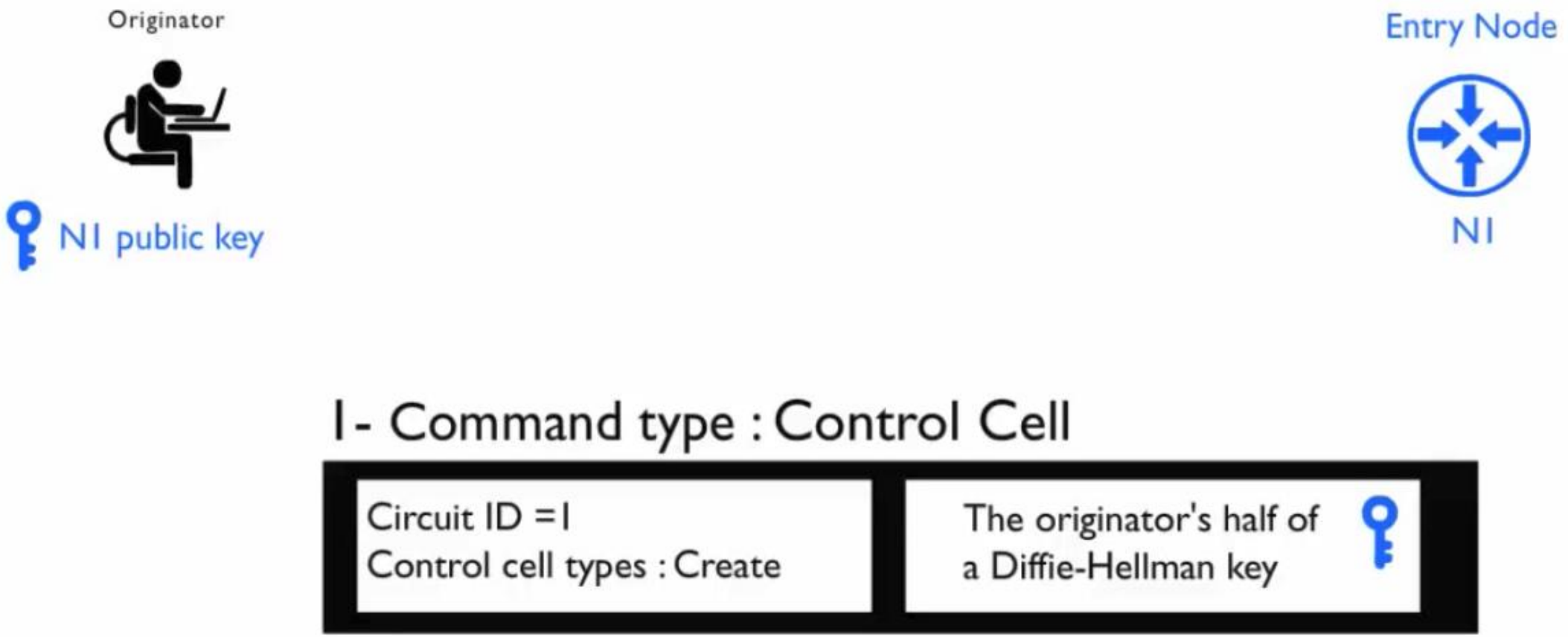
TOR - CELL



TOR - CELL TYPES

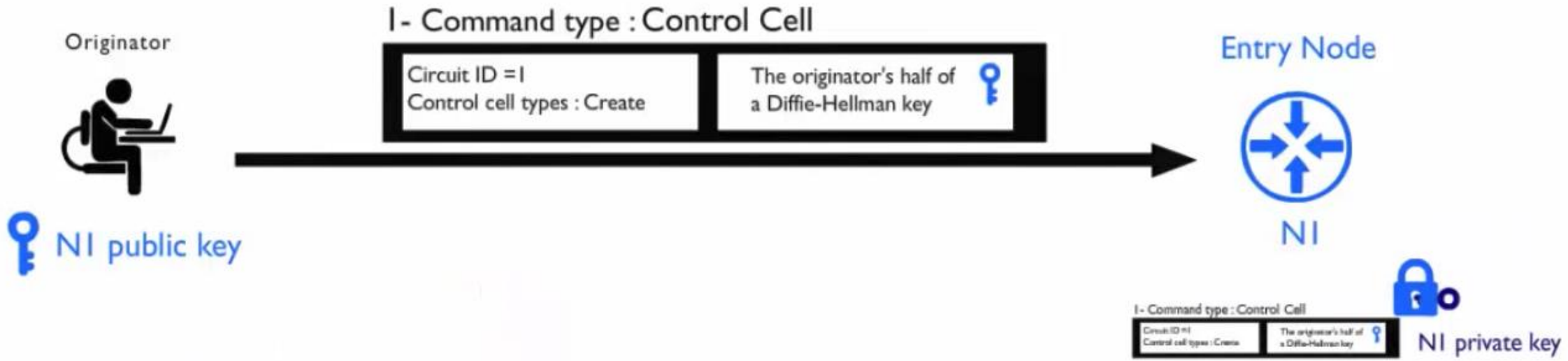
Control Cell	will be interpreted by the receiving node.
Relay Cell	not interpreted by the receiving node, but relayed to another node.

TOR CIRCUIT KEY EXCHANGE

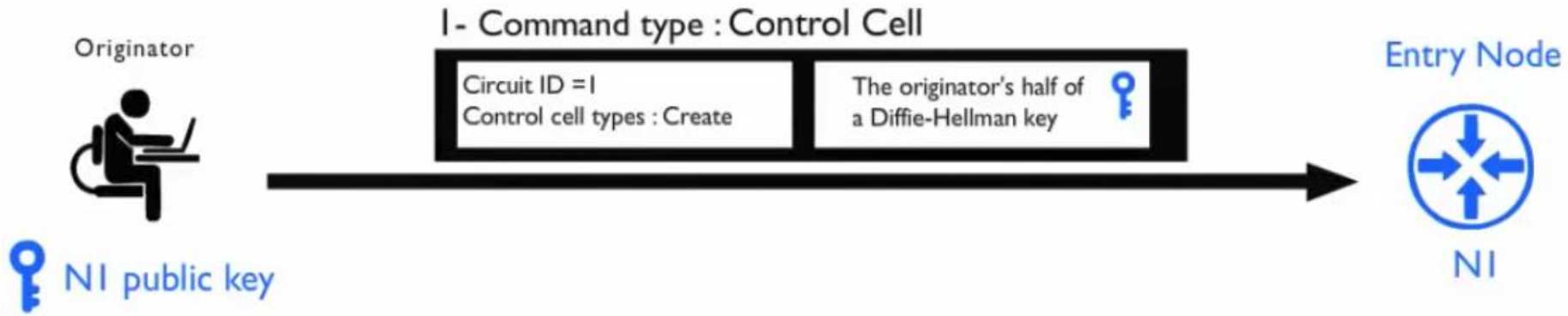


TOR CIRCUIT KEY EXCHANGE (CONTD.)

TOR CIRCUIT KEY EXCHANGE (CONTD.)



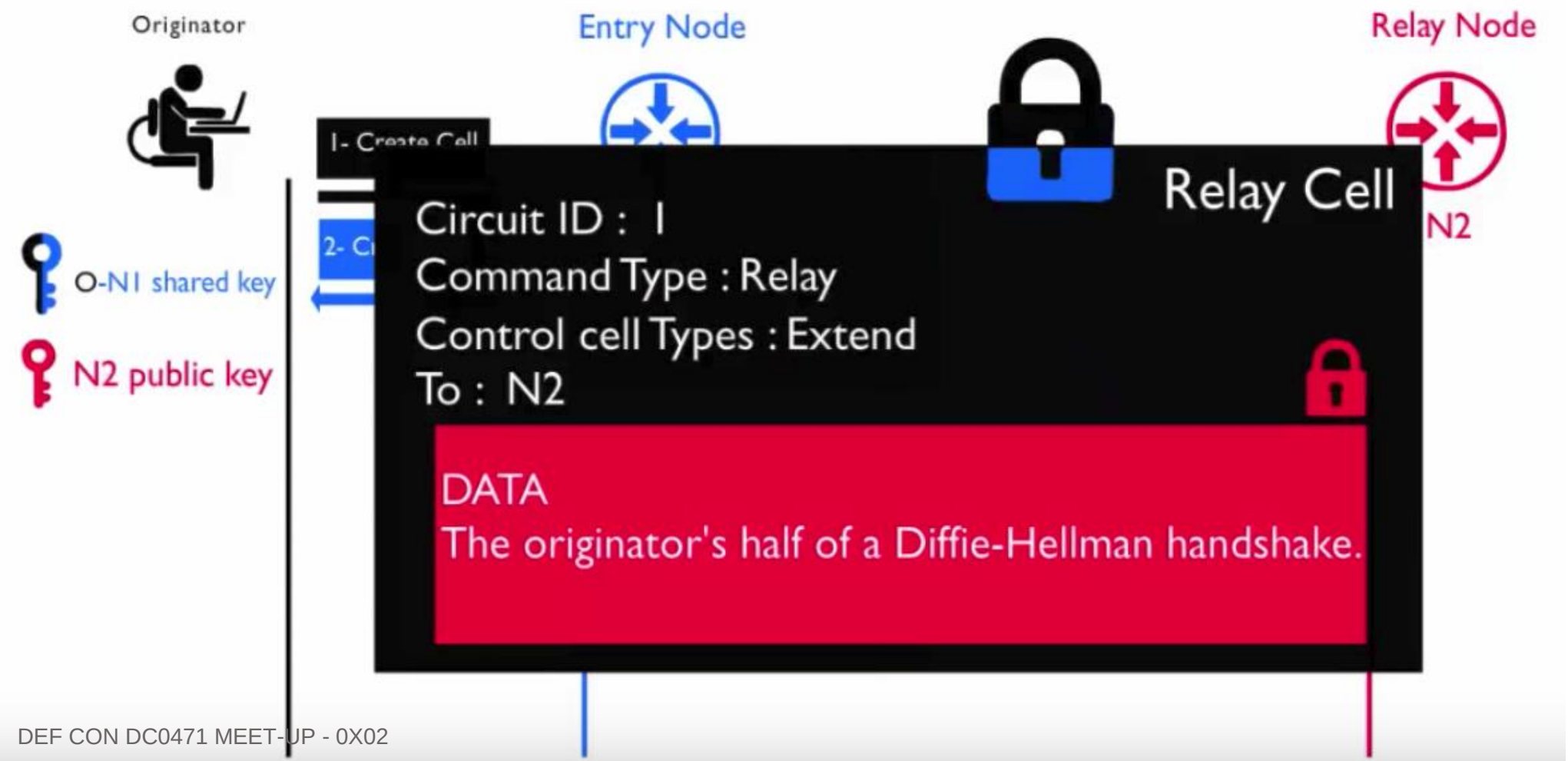
TOR CIRCUIT KEY EXCHANGE (CONTD.)



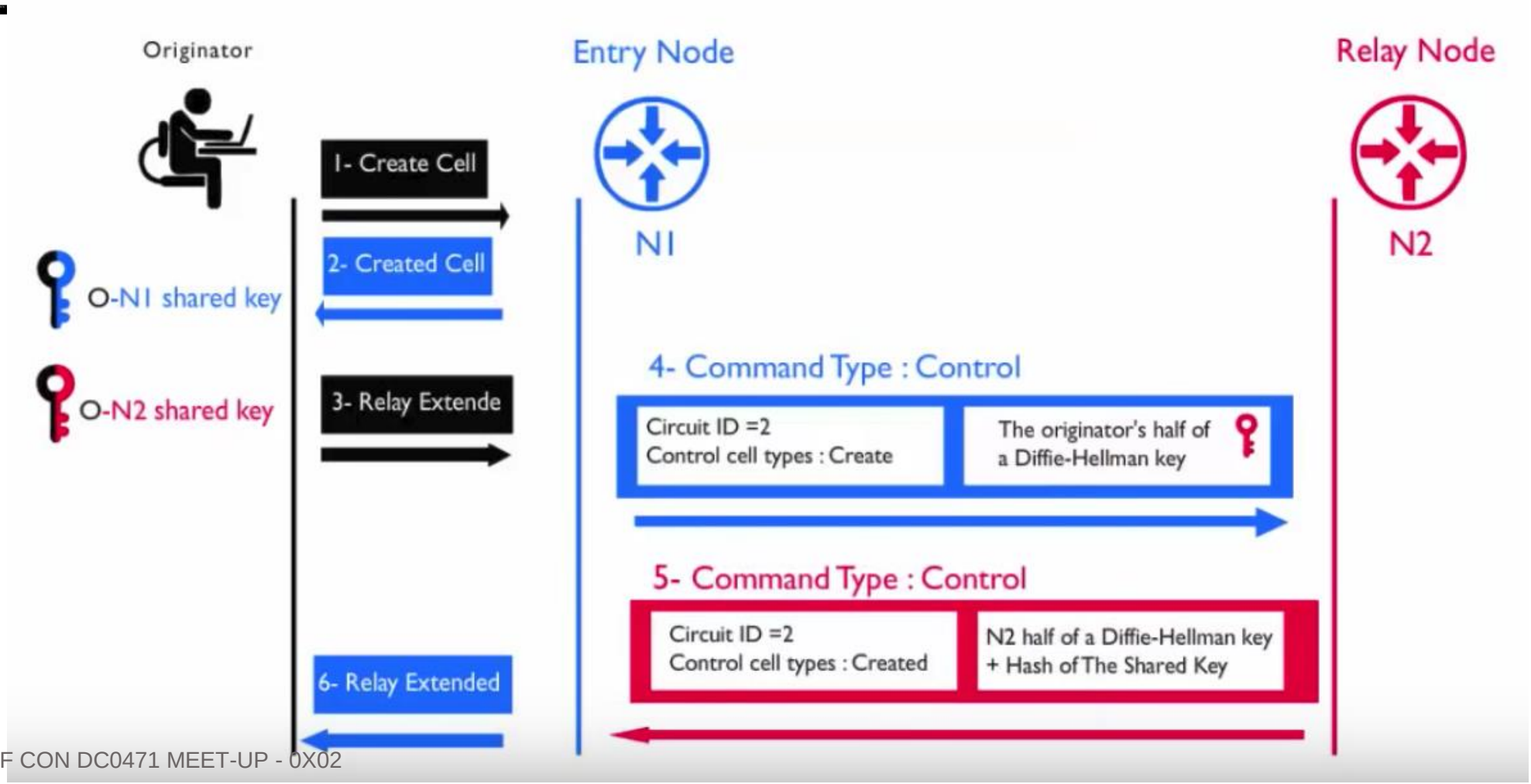
2- Command type : Control Cell

Circuit ID = 1 Control cell types :Created	N1 half of a Diffie-Hellman key Hash of The Shared Key

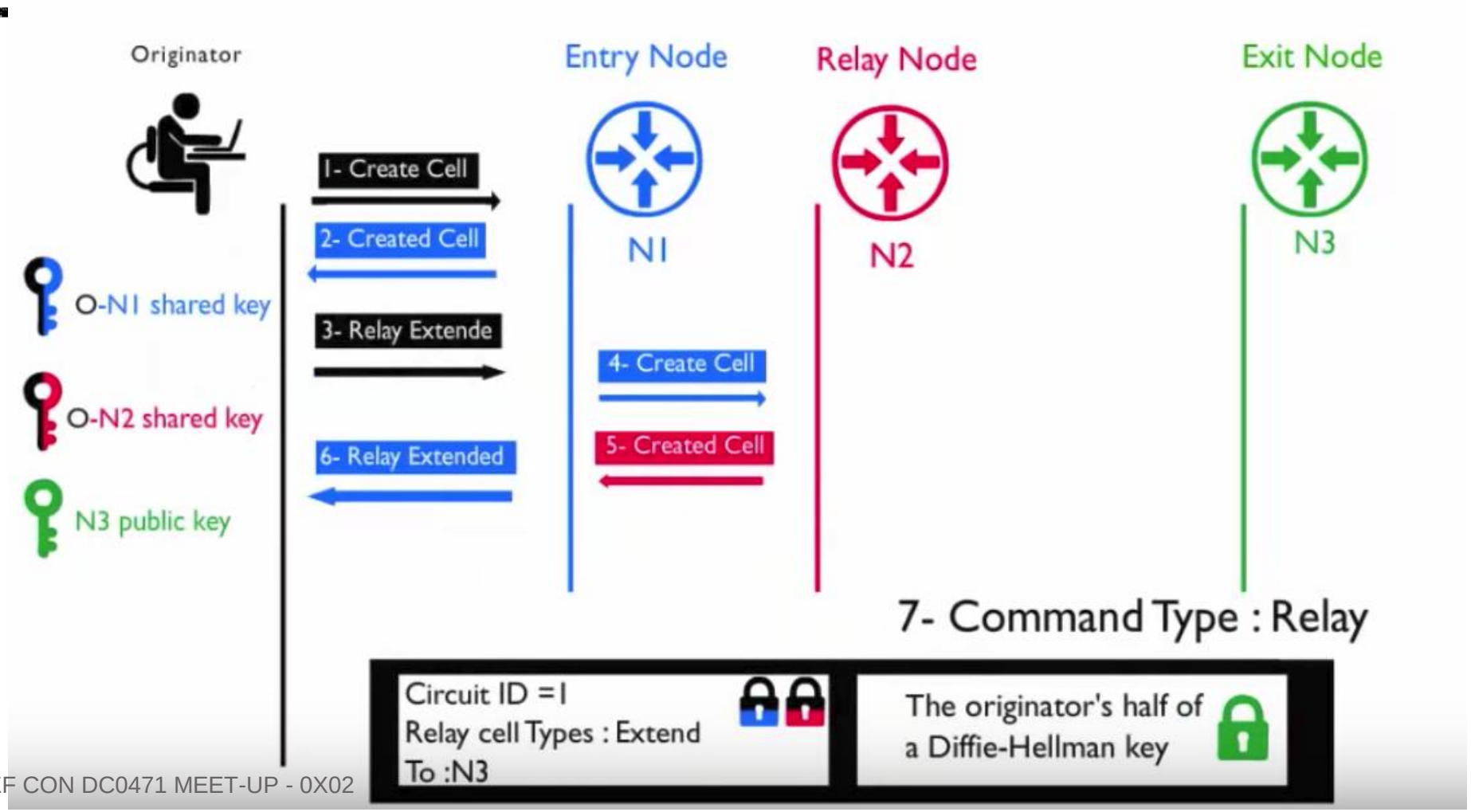
TOR CIRCUIT KEY EXCHANGE (CONTD.)



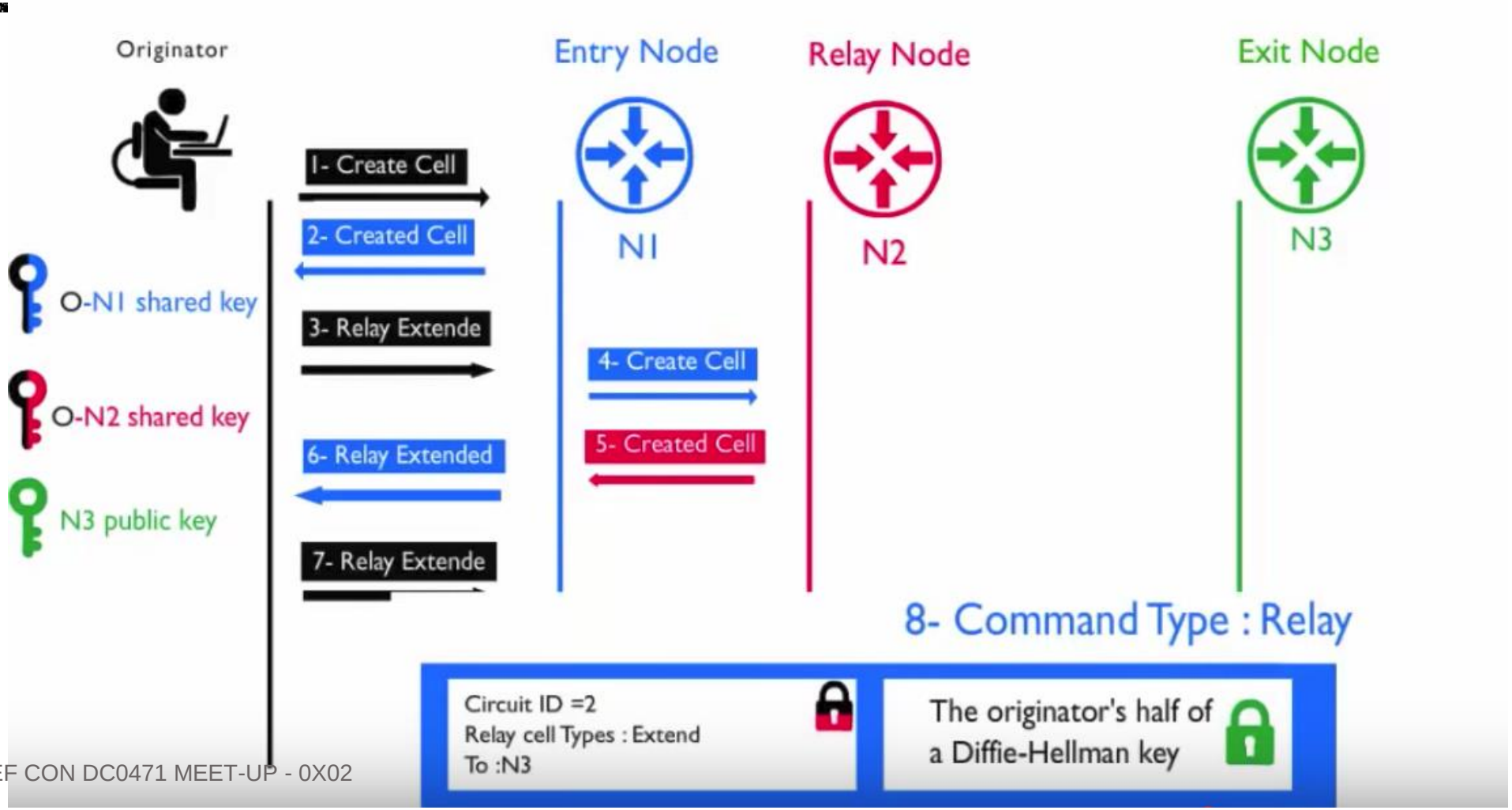
TOR CIRCUIT KEY EXCHANGE (CONTD.)



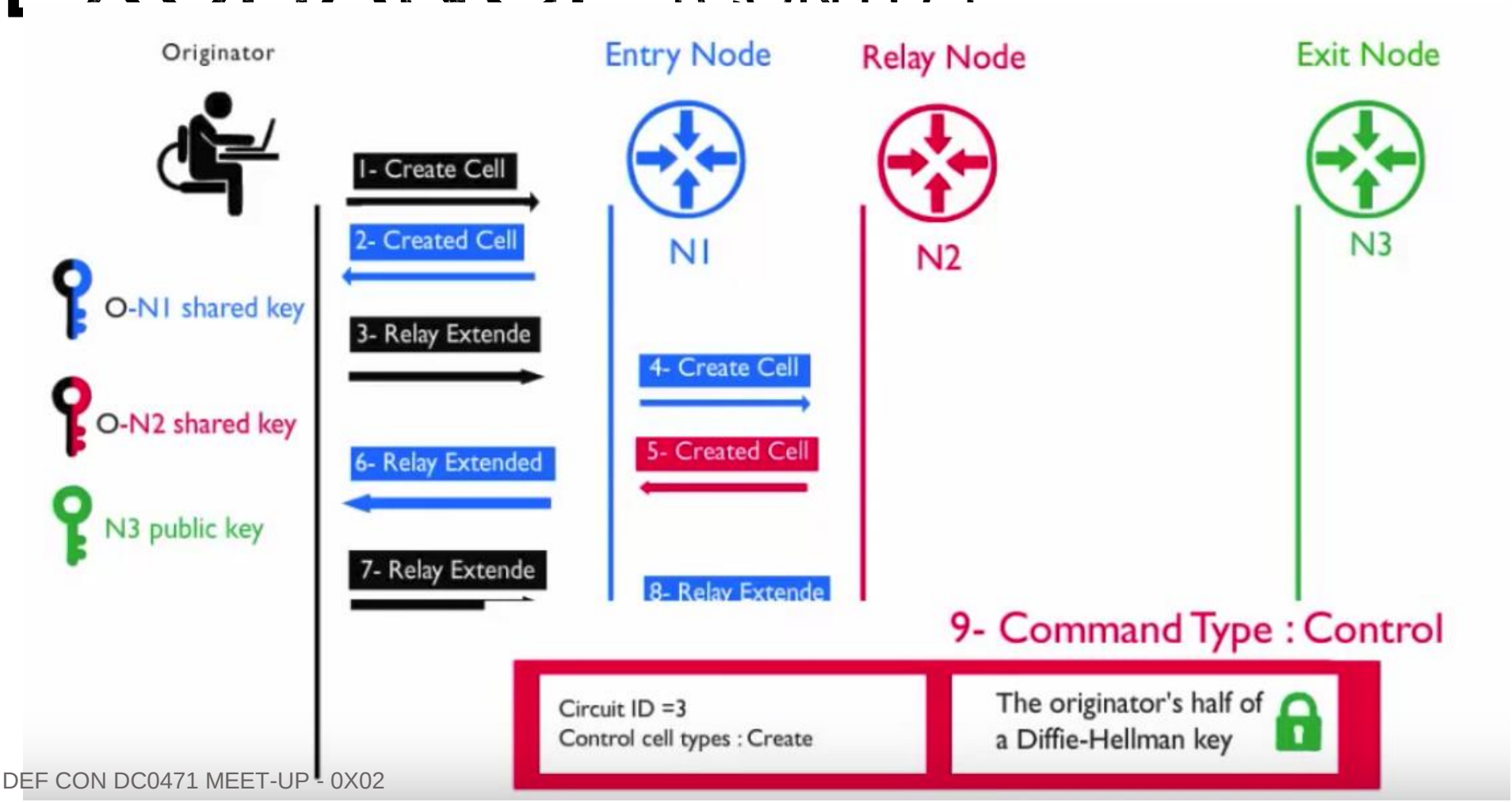
TOR CIRCUIT KEY EXCHANGE (CONTD.)



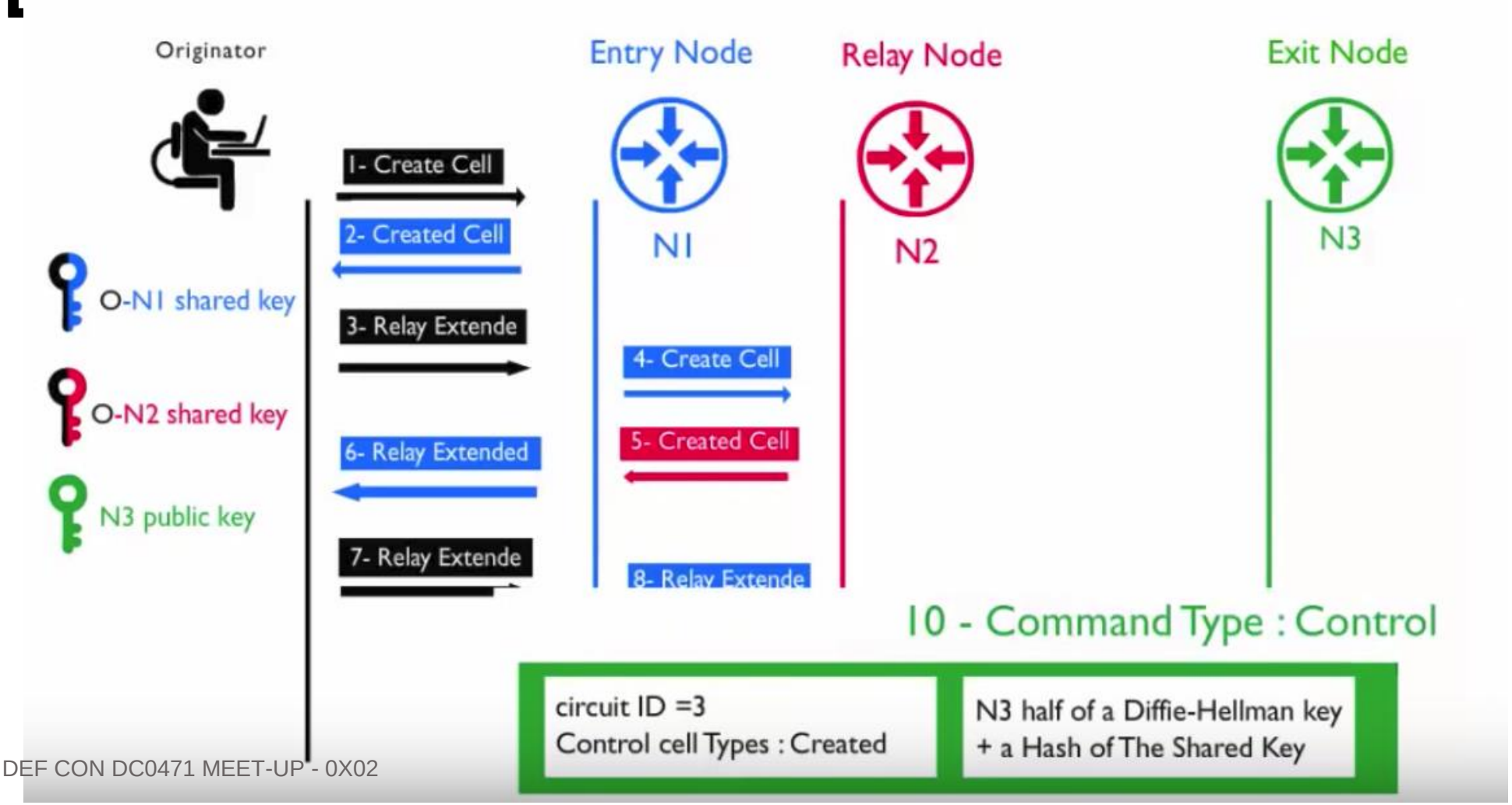
TOR CIRCUIT KEY EXCHANGE (CONTD.)



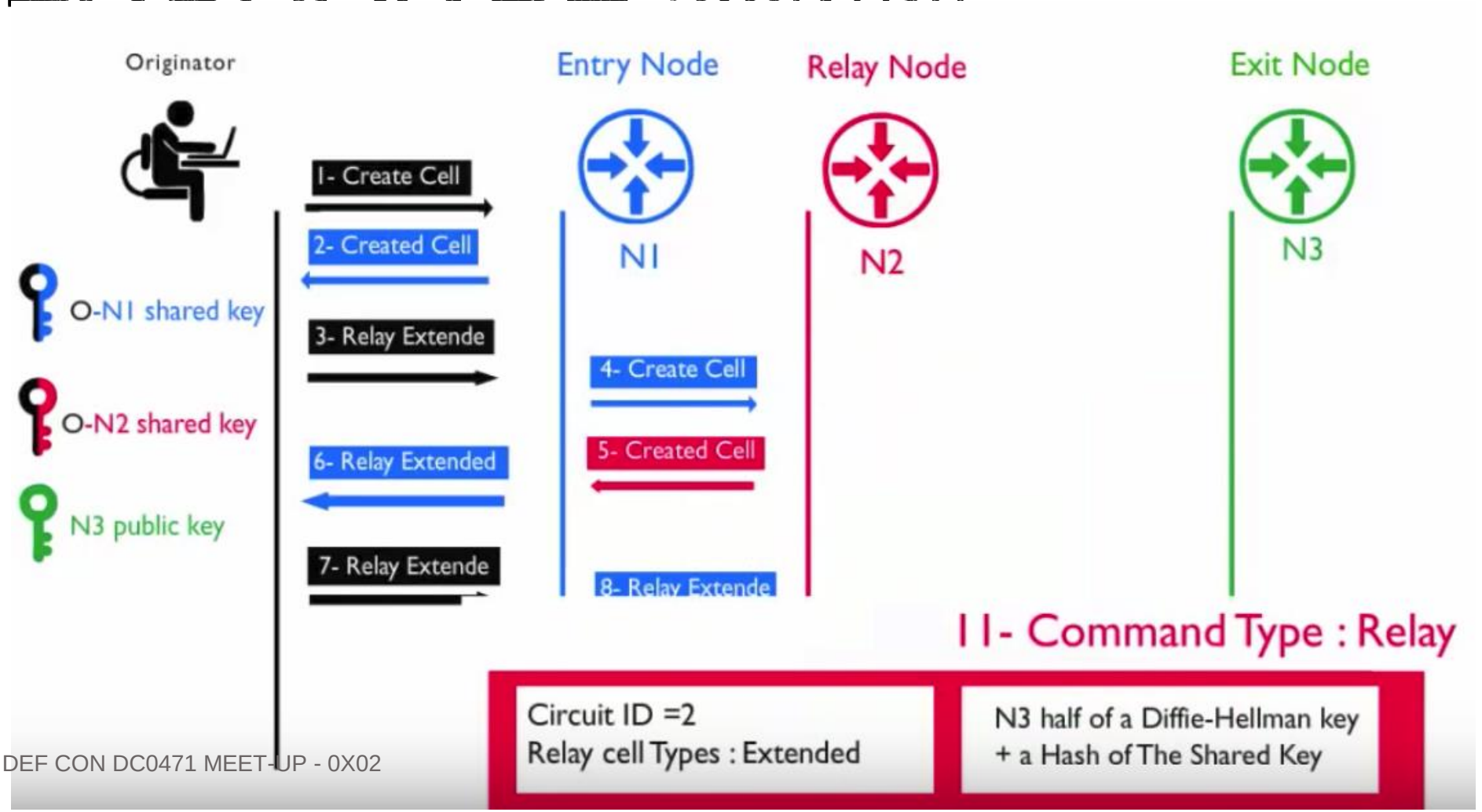
TOR CIRCUIT KEY EXCHANGE (CONTD.)



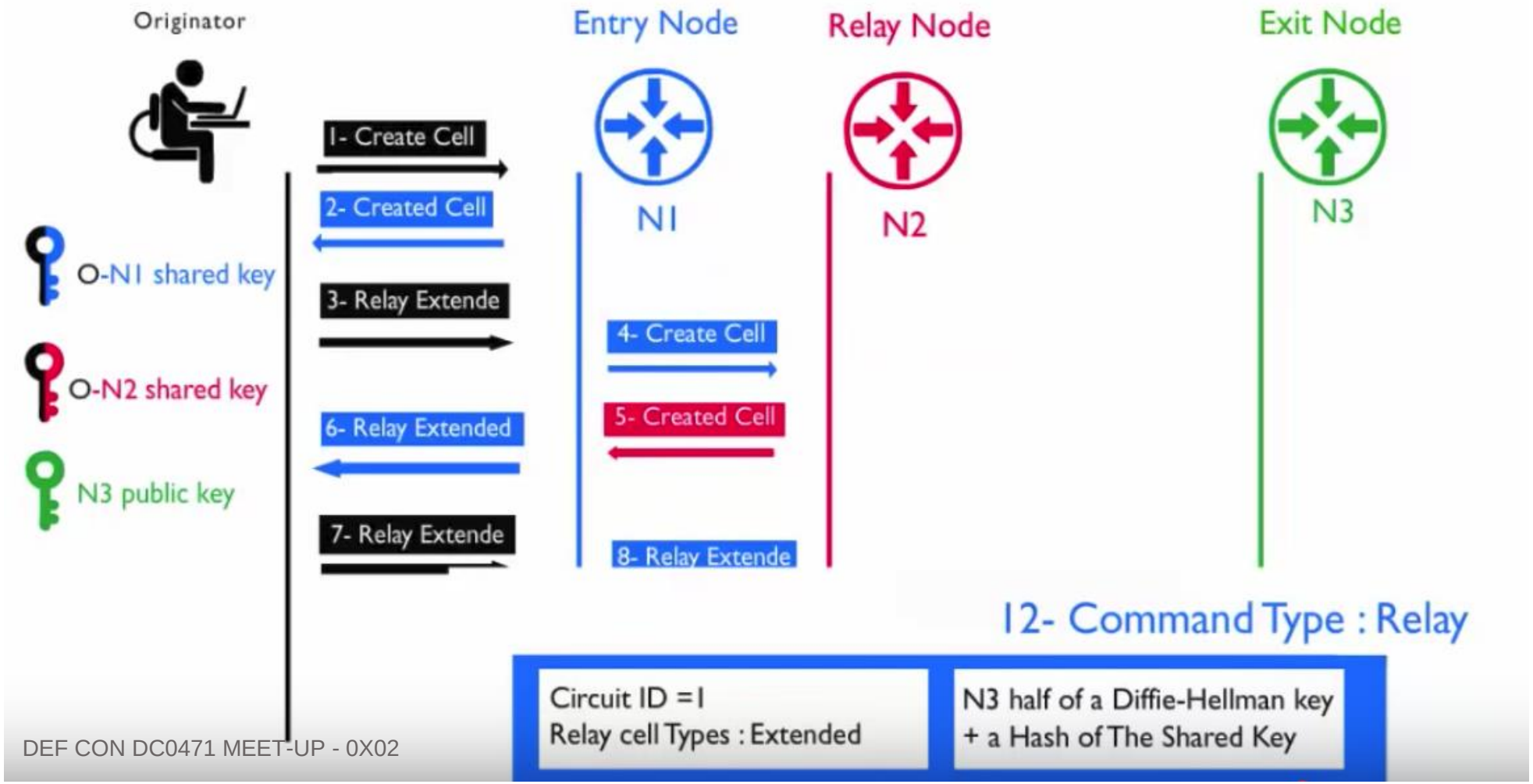
TOR CIRCUIT KEY EXCHANGE (CONTD.)



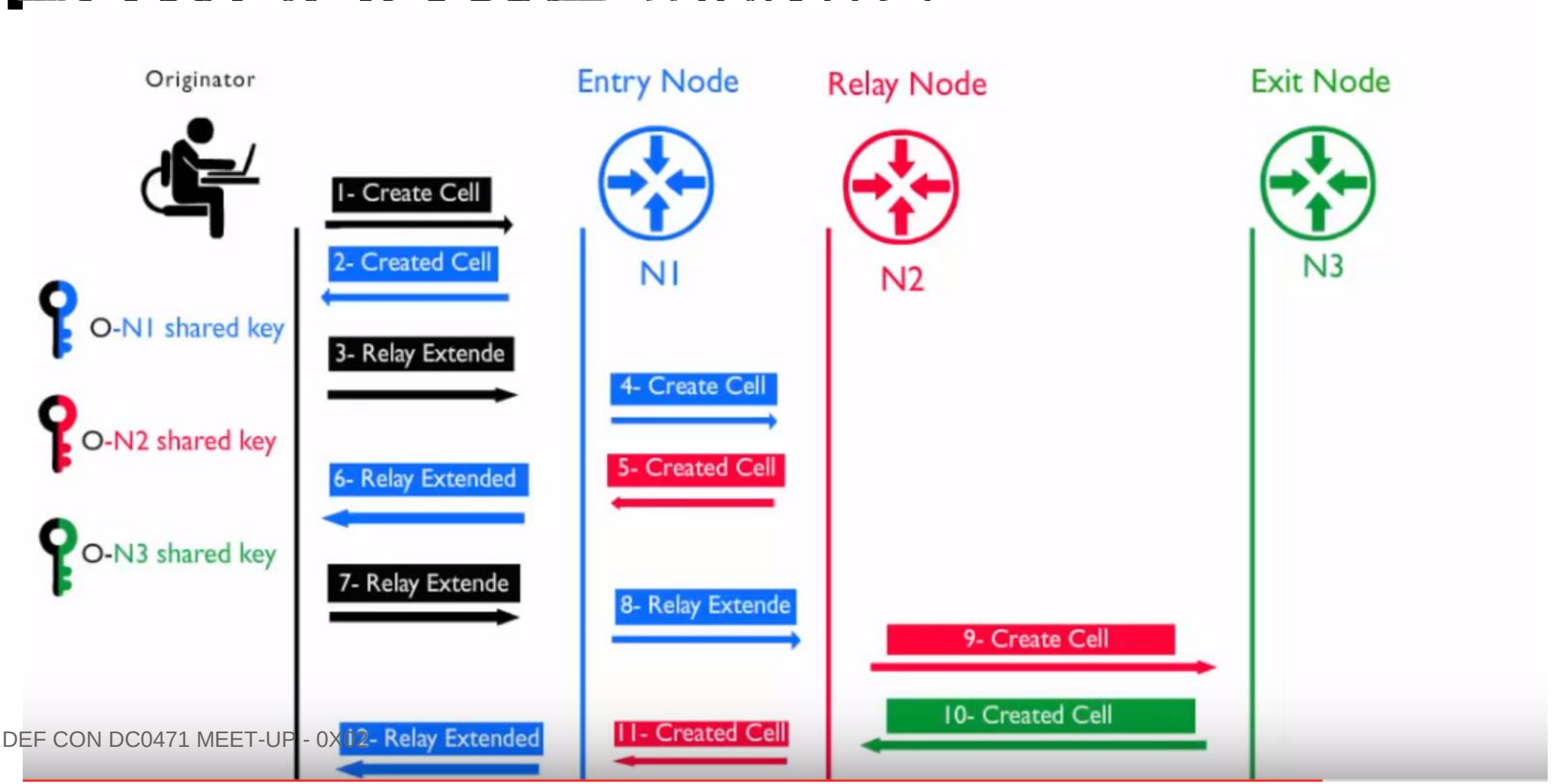
TOR CIRCUIT KEY EXCHANGE (CONTD.)



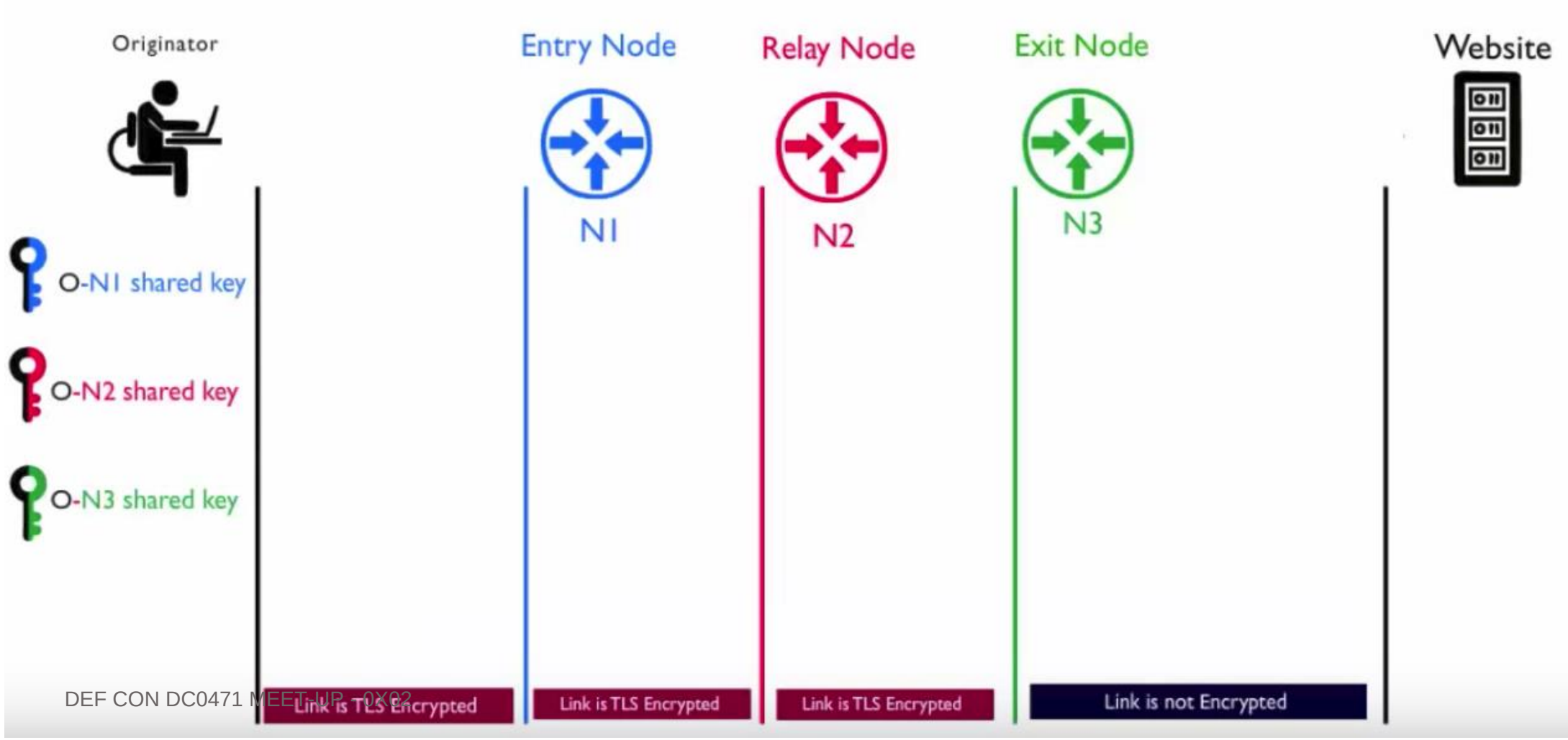
TOR CIRCUIT KEY EXCHANGE (CONTD.)



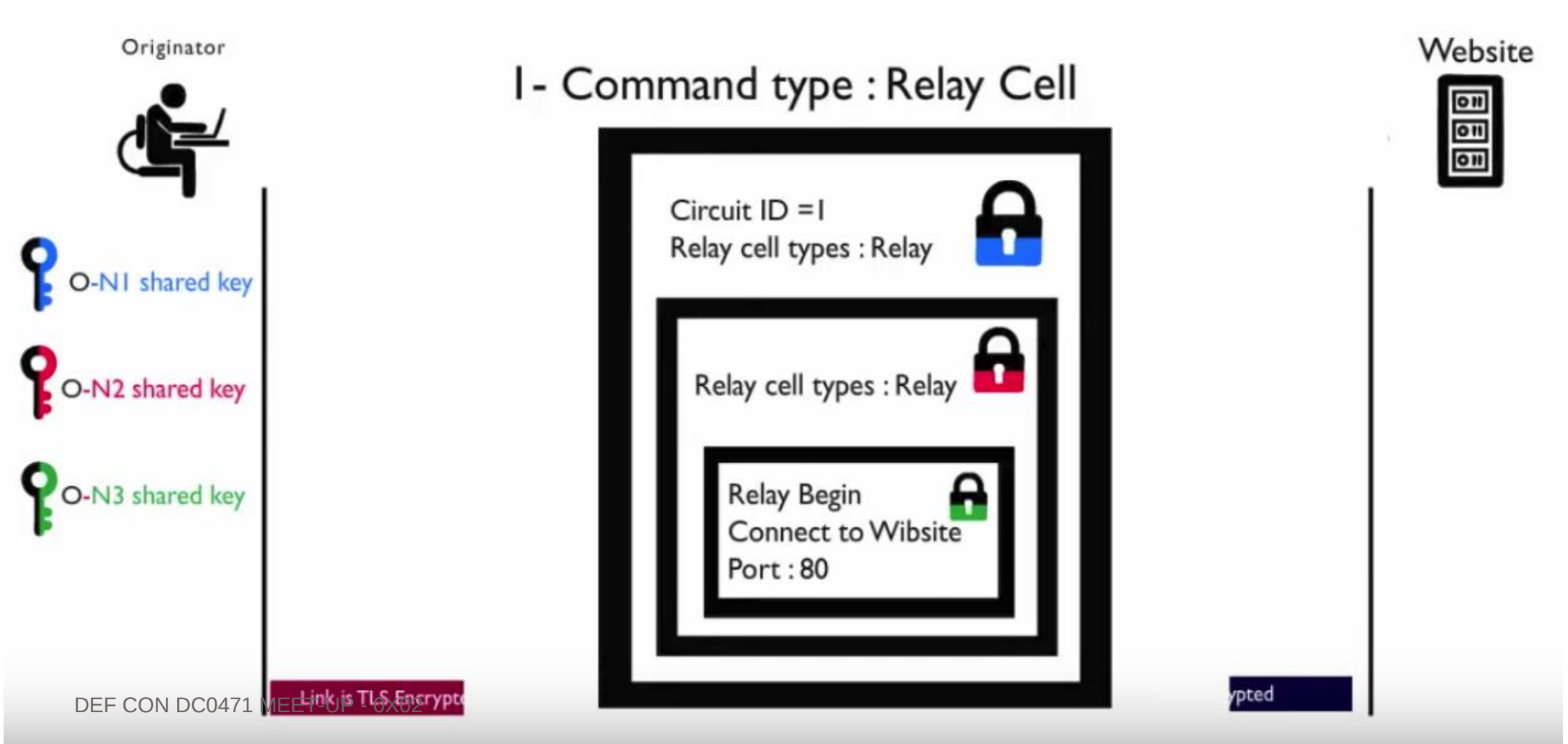
TOR CIRCUIT KEY EXCHANGE (CONTD.)



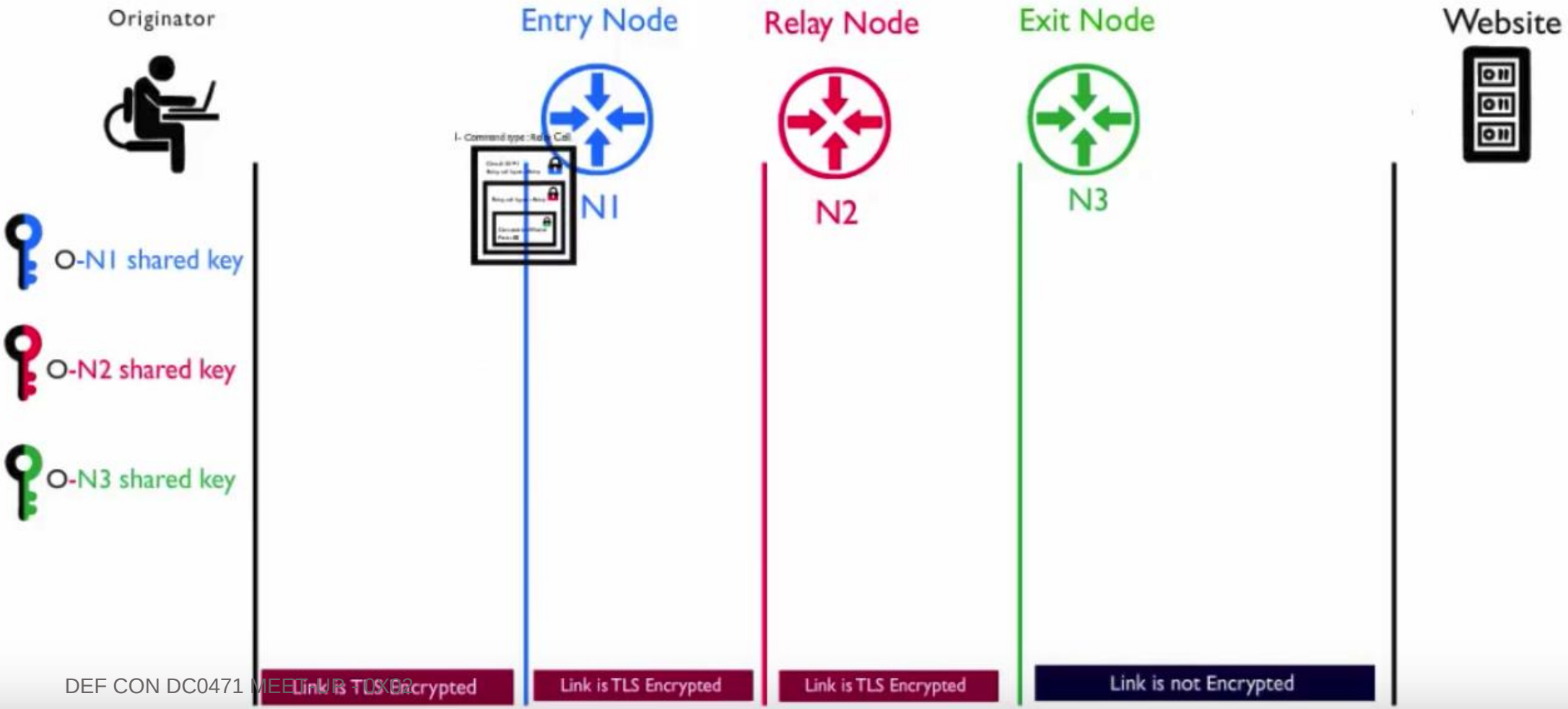
ANONYMOUS WEB PAGE



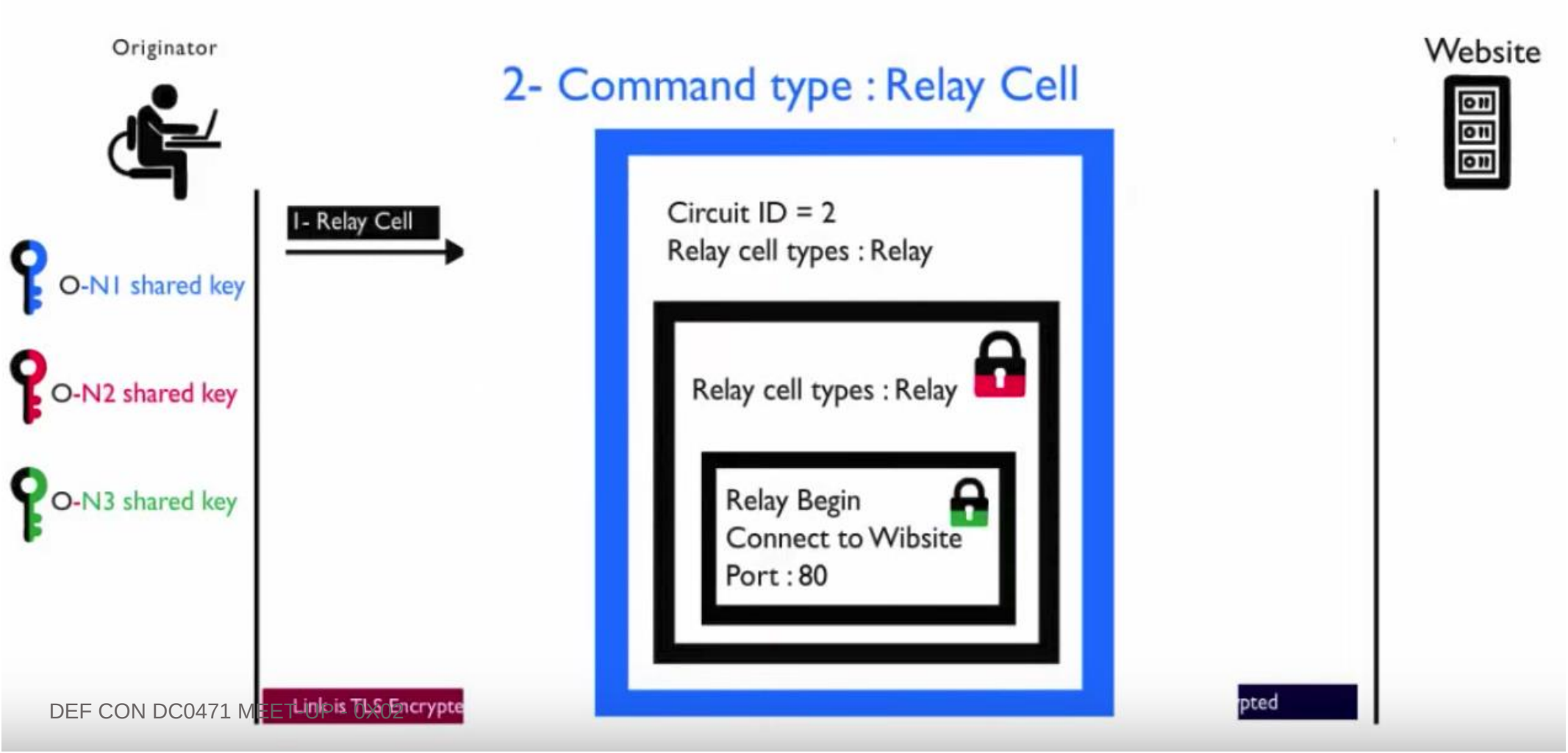
ANONYMOUS WEB PAGE (CONTD.)



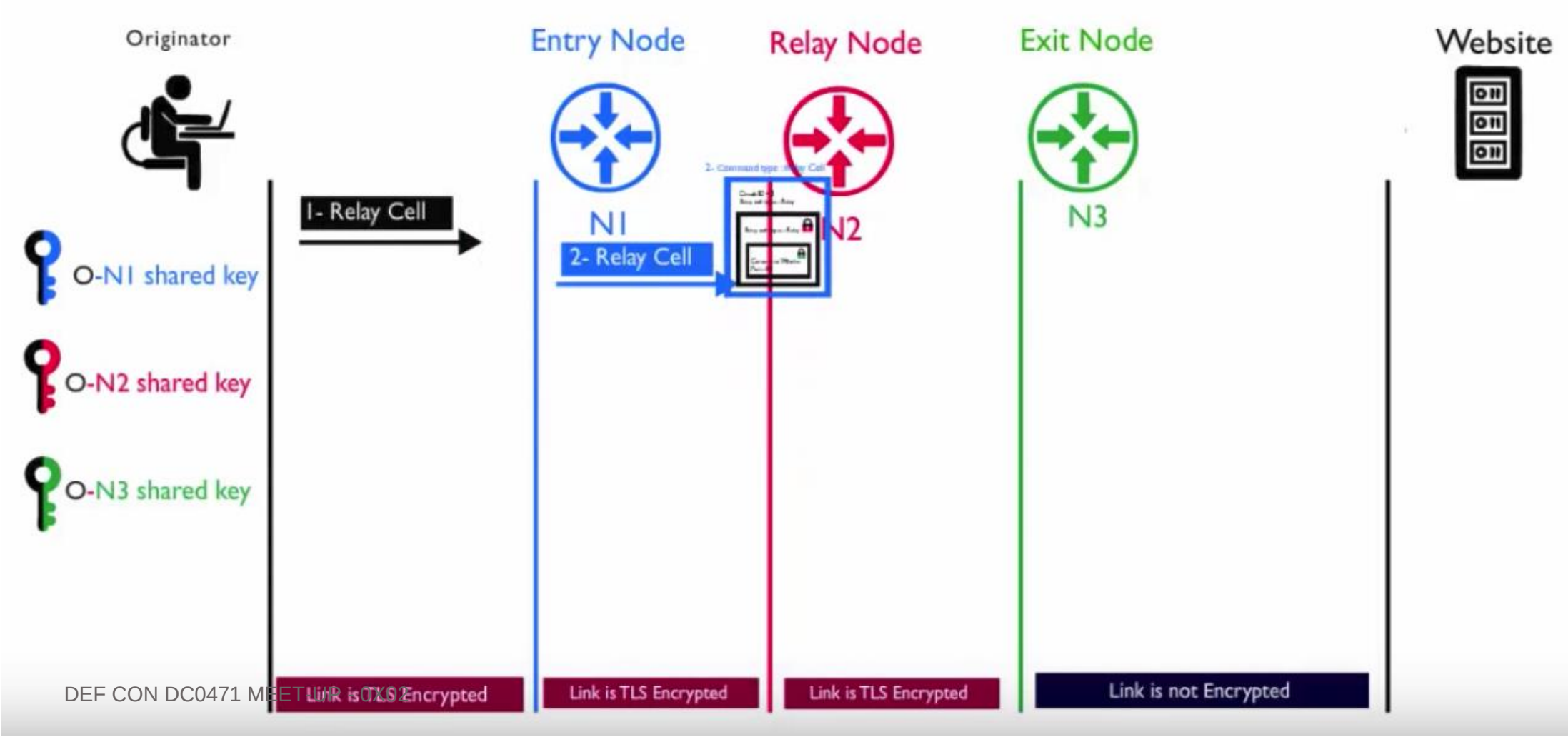
ANONYMOUS WEB PAGE (CONTD.)



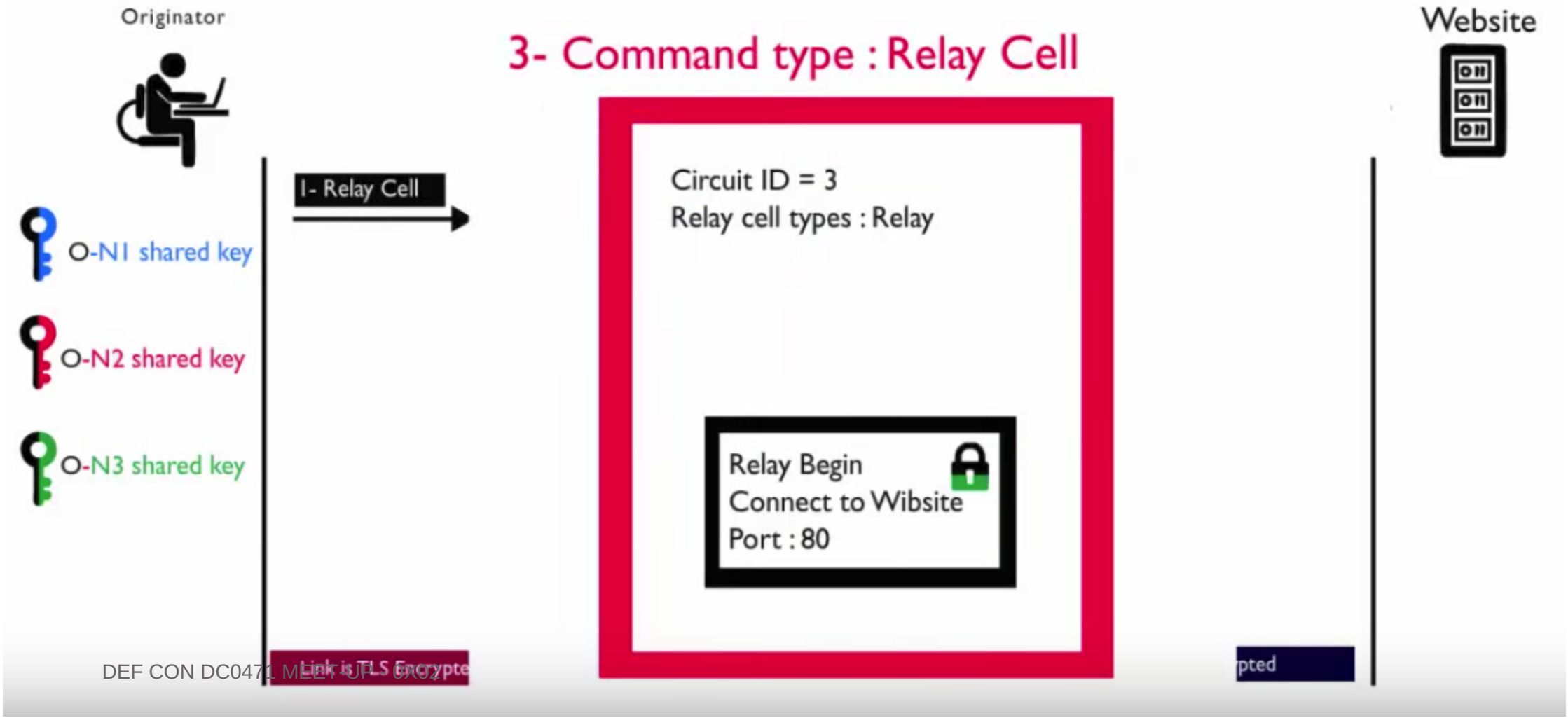
ANONYMOUS WEB PAGE (CONTD.)



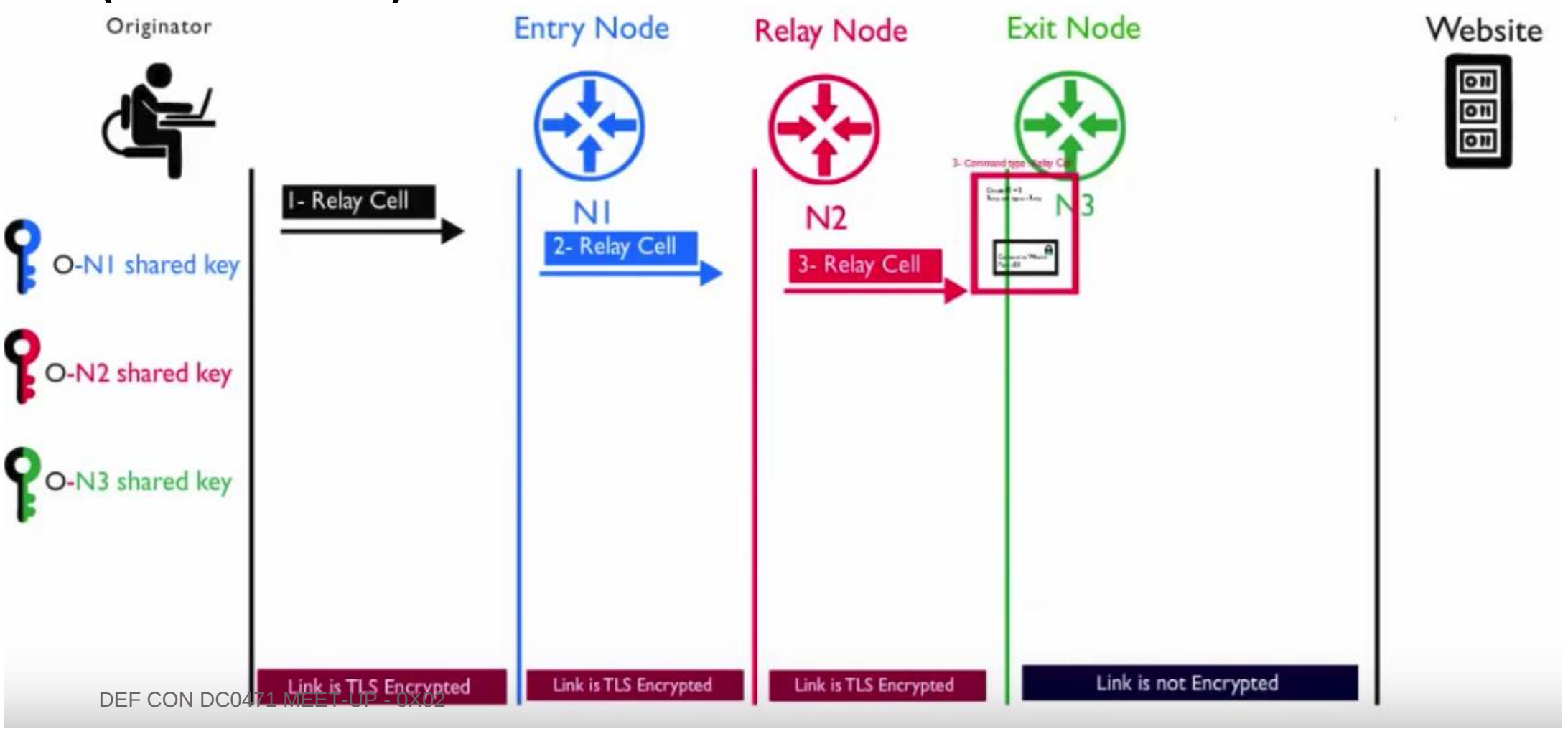
ANONYMOUS WEB PAGE (CONTD.)



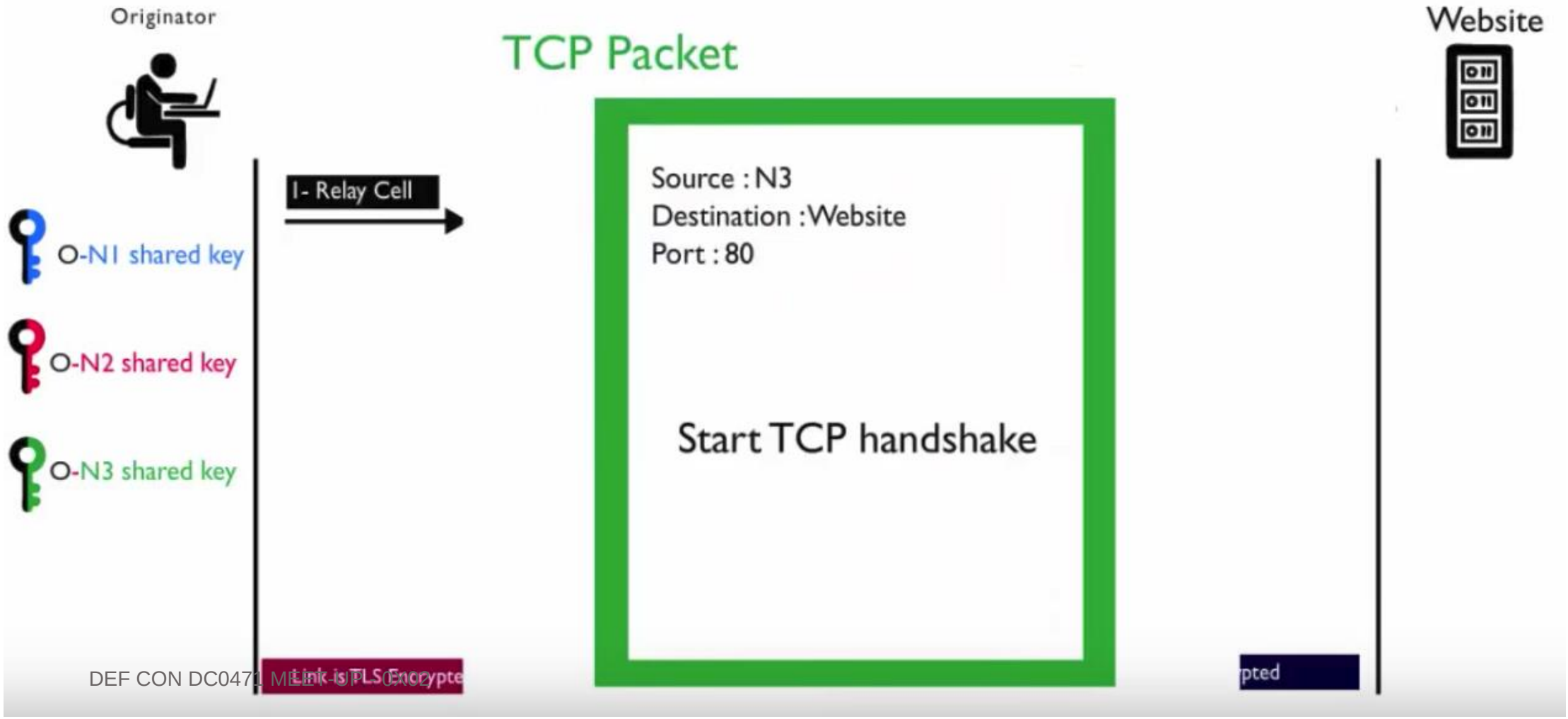
ANONYMOUS WEB PAGE (CONTD.)



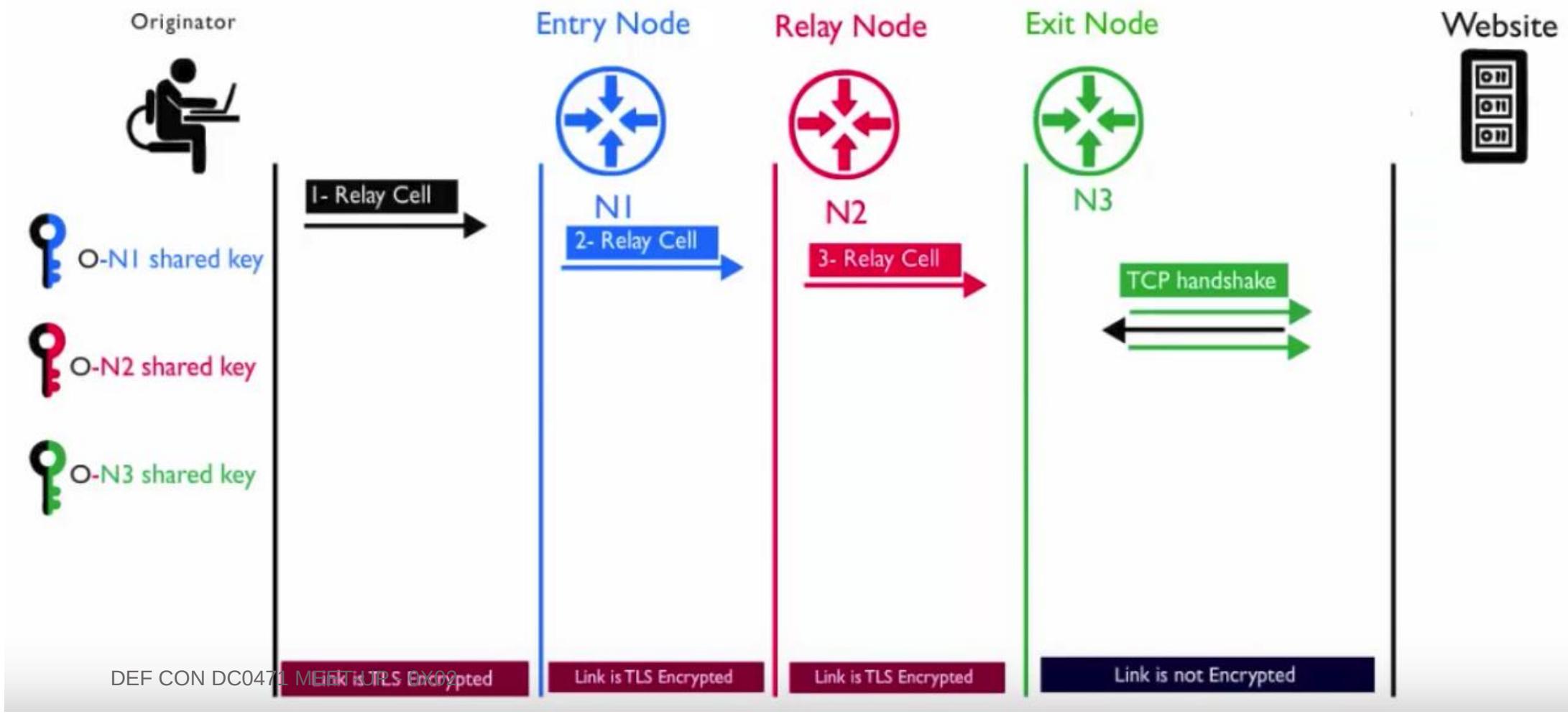
ANONYMOUS WEB PAGE (CONTD.)



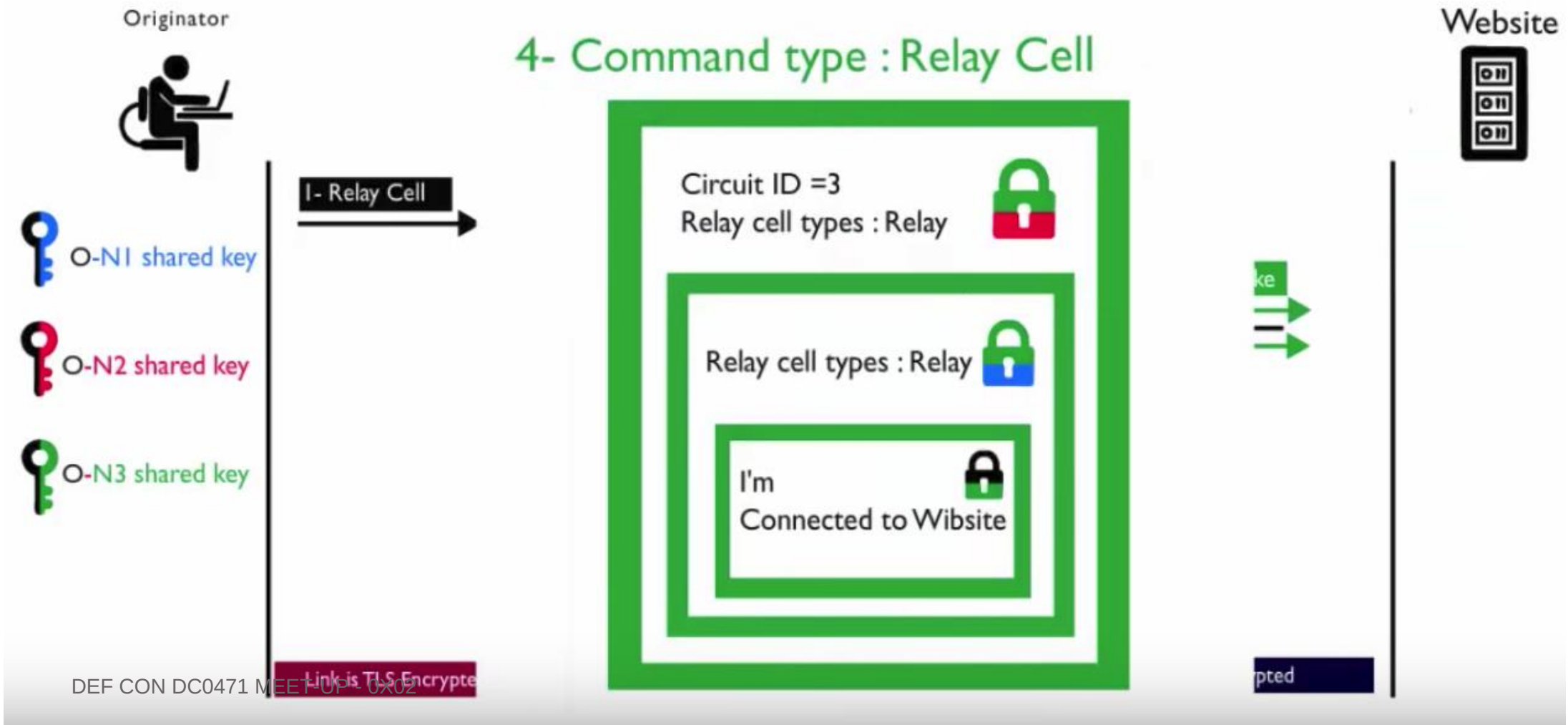
ANONYMOUS WEB PAGE (CONTD.)



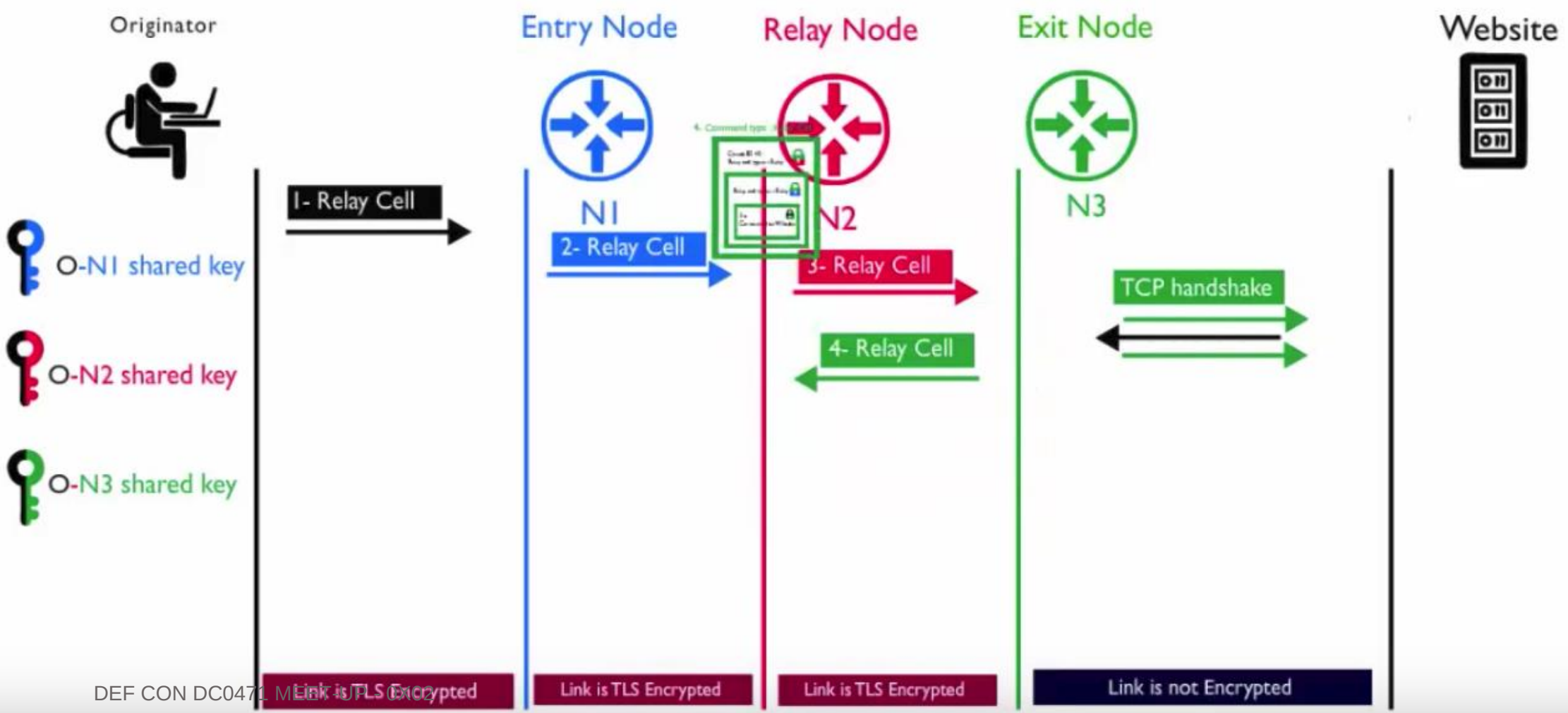
ANONYMOUS WEB PAGE (CONTD.)



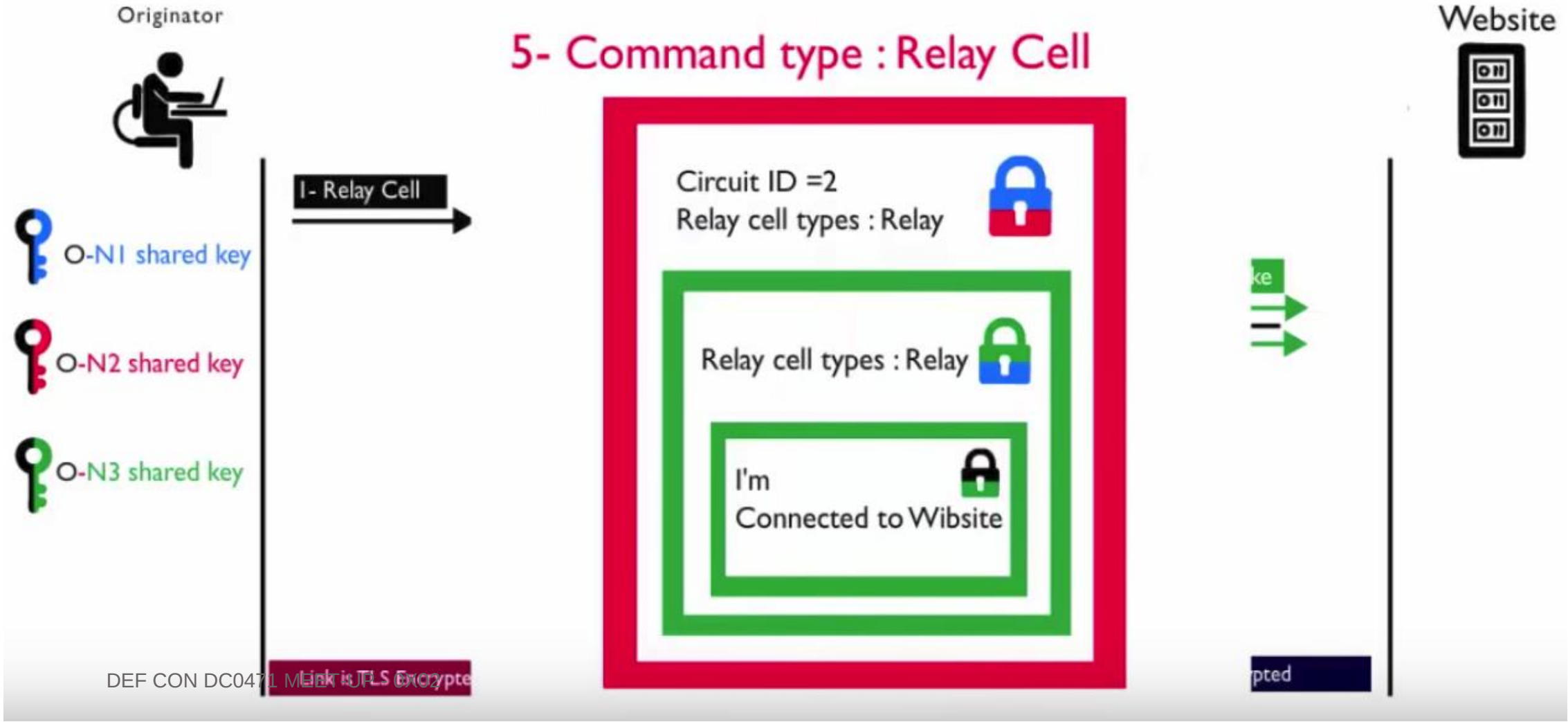
ANONYMOUS WEB PAGE (CONTD.)



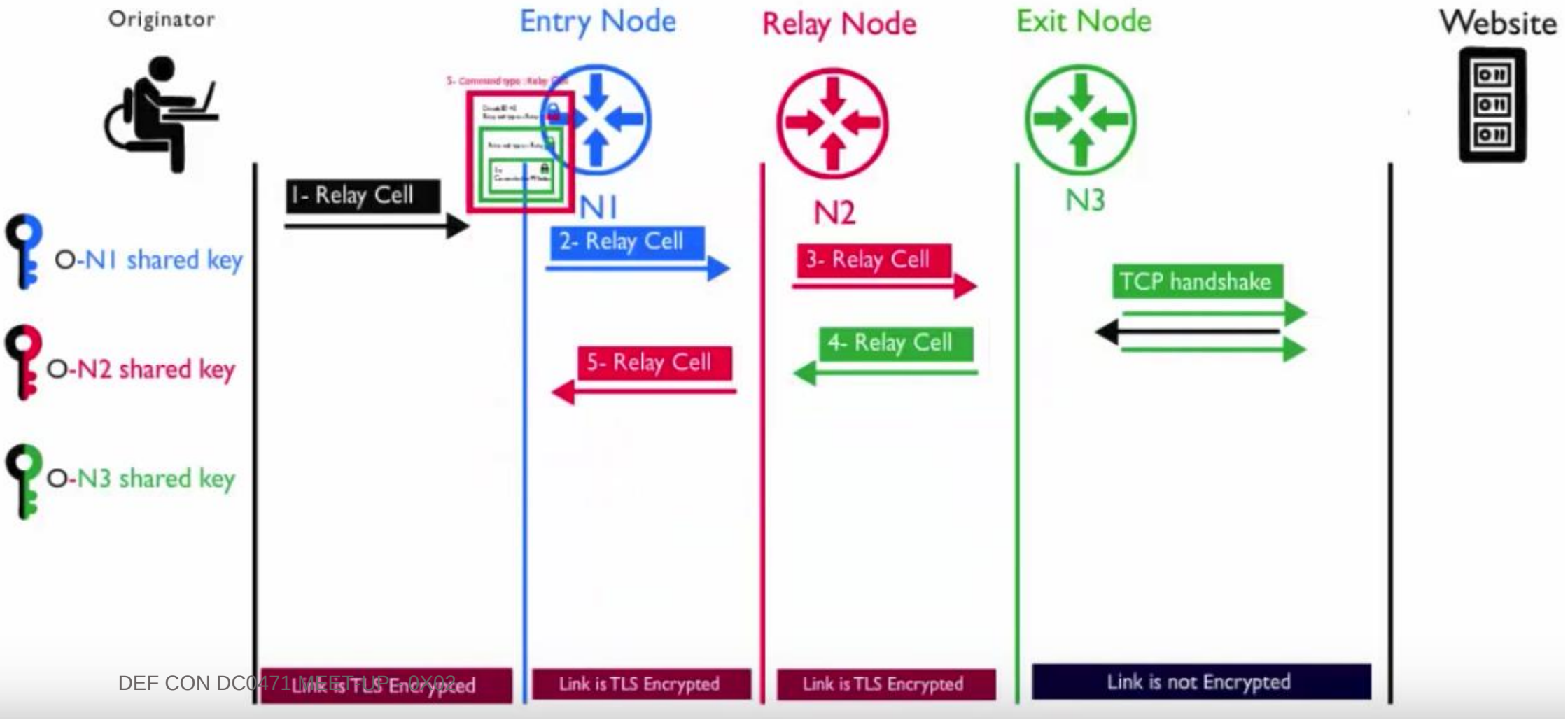
ANONYMOUS WEB PAGE (CONTD.)



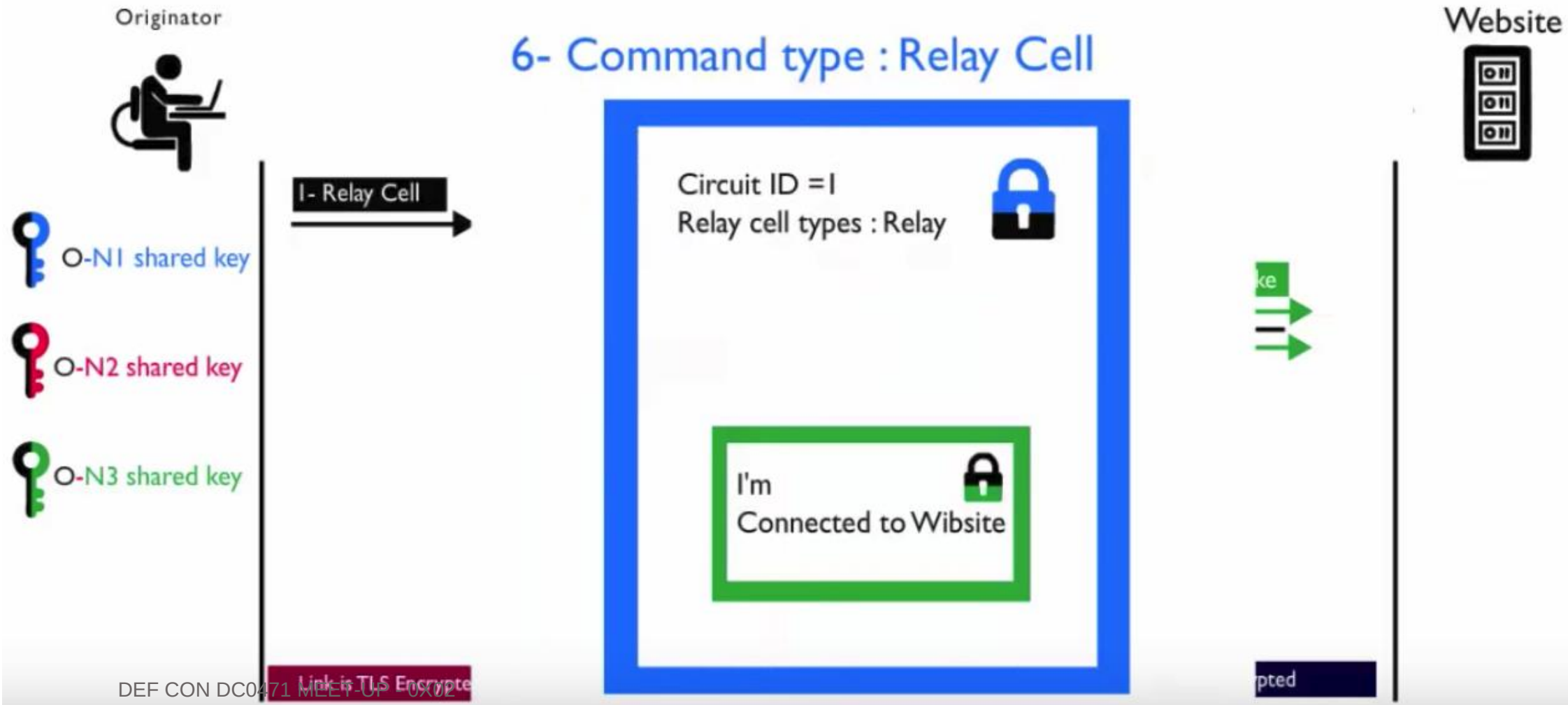
ANONYMOUS WEB PAGE (CONTD.)



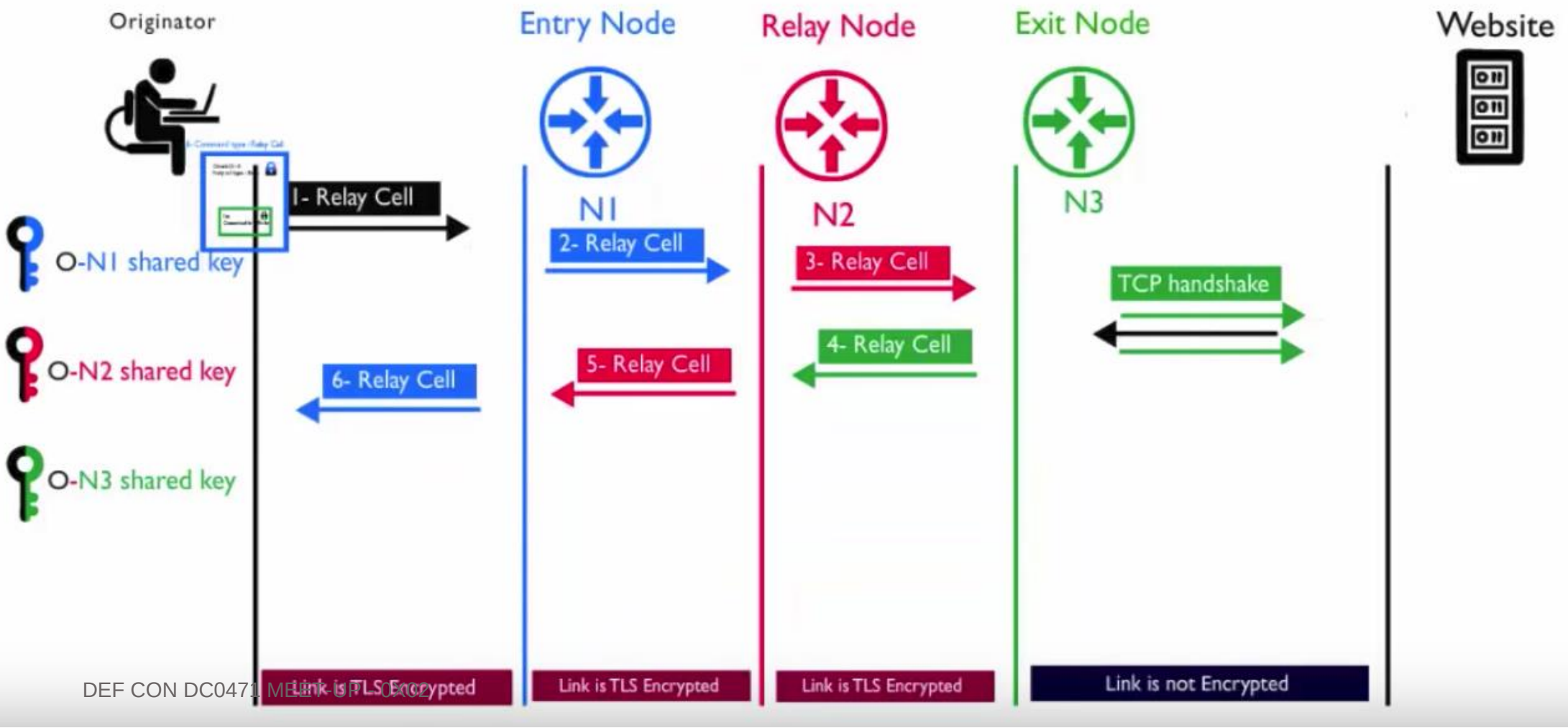
ANONYMOUS WEB PAGE (CONTD.)



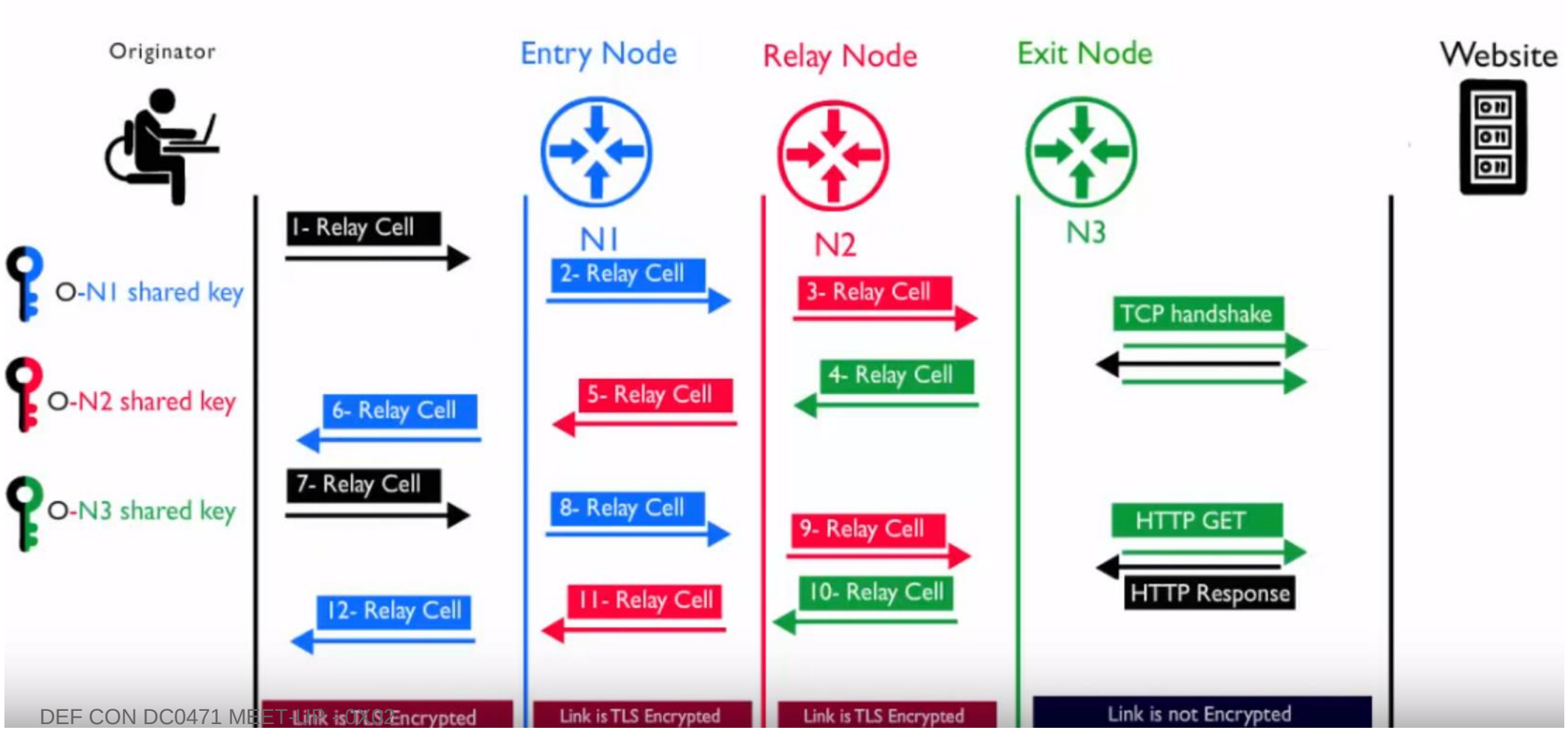
ANONYMOUS WEB PAGE (CONTD.)



ANONYMOUS WEB PAGE (CONTD.)



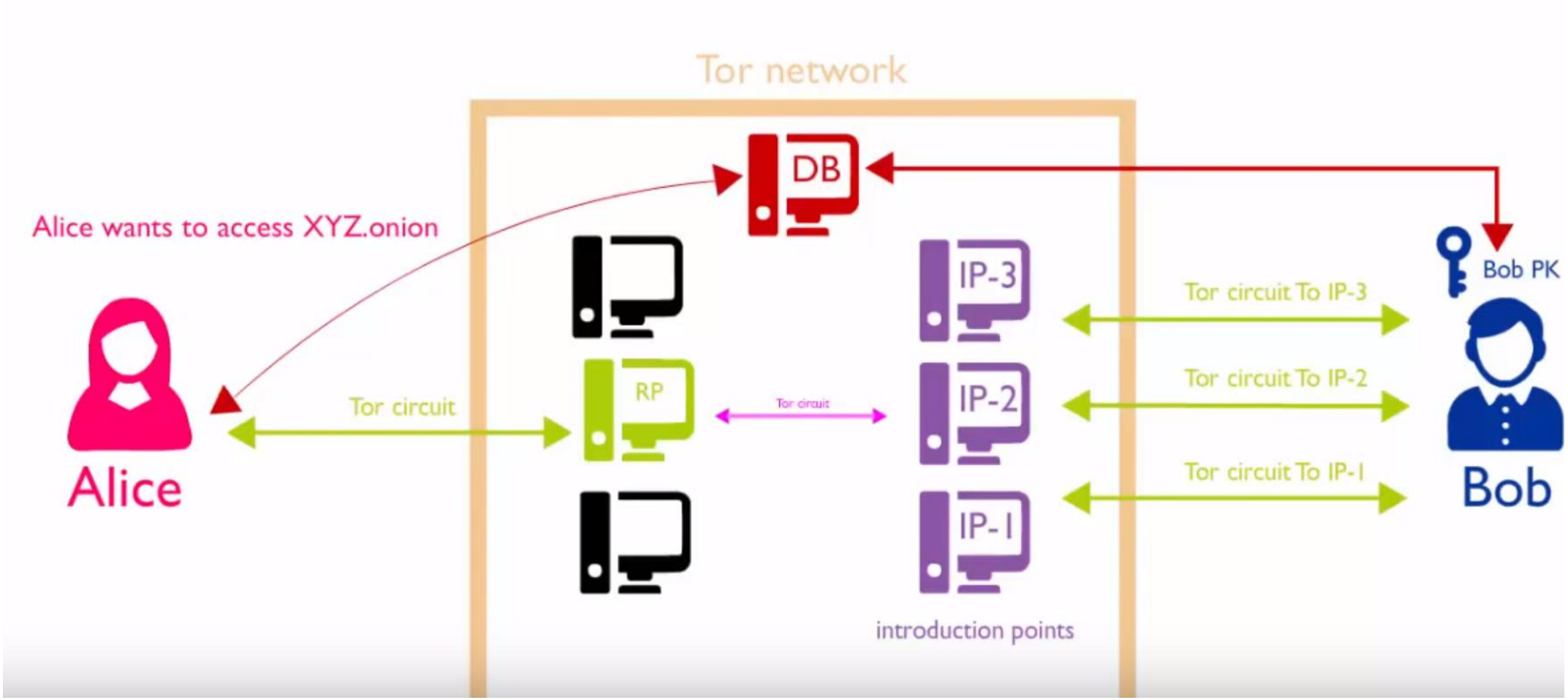
ANONYMOUS WEB PAGE (CONTD.)



TOR - ONION SERVICES

- ToR makes it possible for users to hide their locations while offering various kinds of services, such as web publishing or an instant messaging server.
- Using ToR "**rendezvous points**", other ToR users can connect to these onion services, each without knowing the other's network identity.
- A hidden service needs to advertise its existence in the ToR network before clients will be able to contact it.
- The service randomly picks some relays, builds circuits to them, and asks them to act as ***introduction points*** by telling them its public key.
- By using a full ToR circuit, it's hard for anyone to associate an introduction point with the hidden server's IP address.

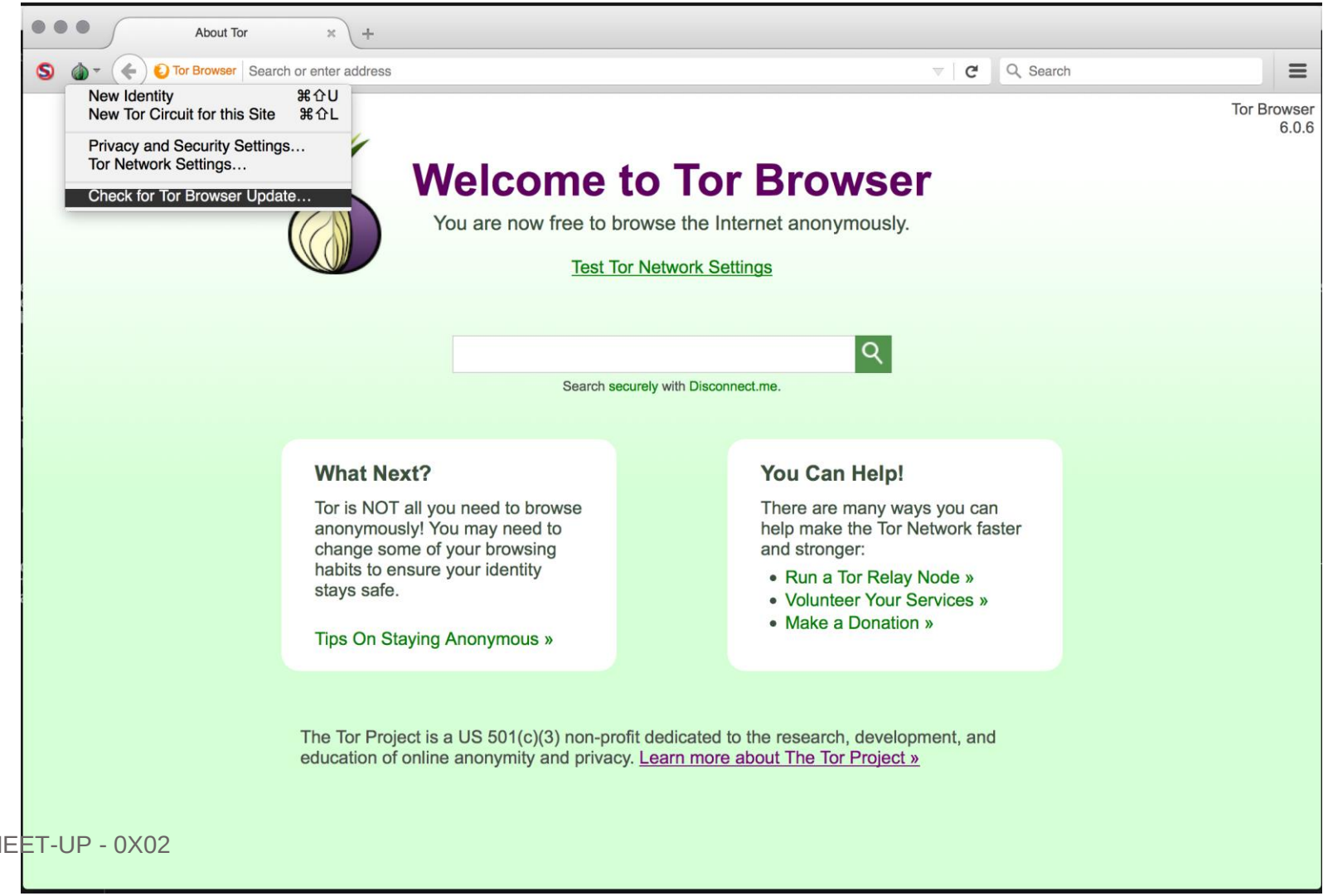
ONION SERVICE PROTOCOL



HOSTING A WEBSITE IN TOR

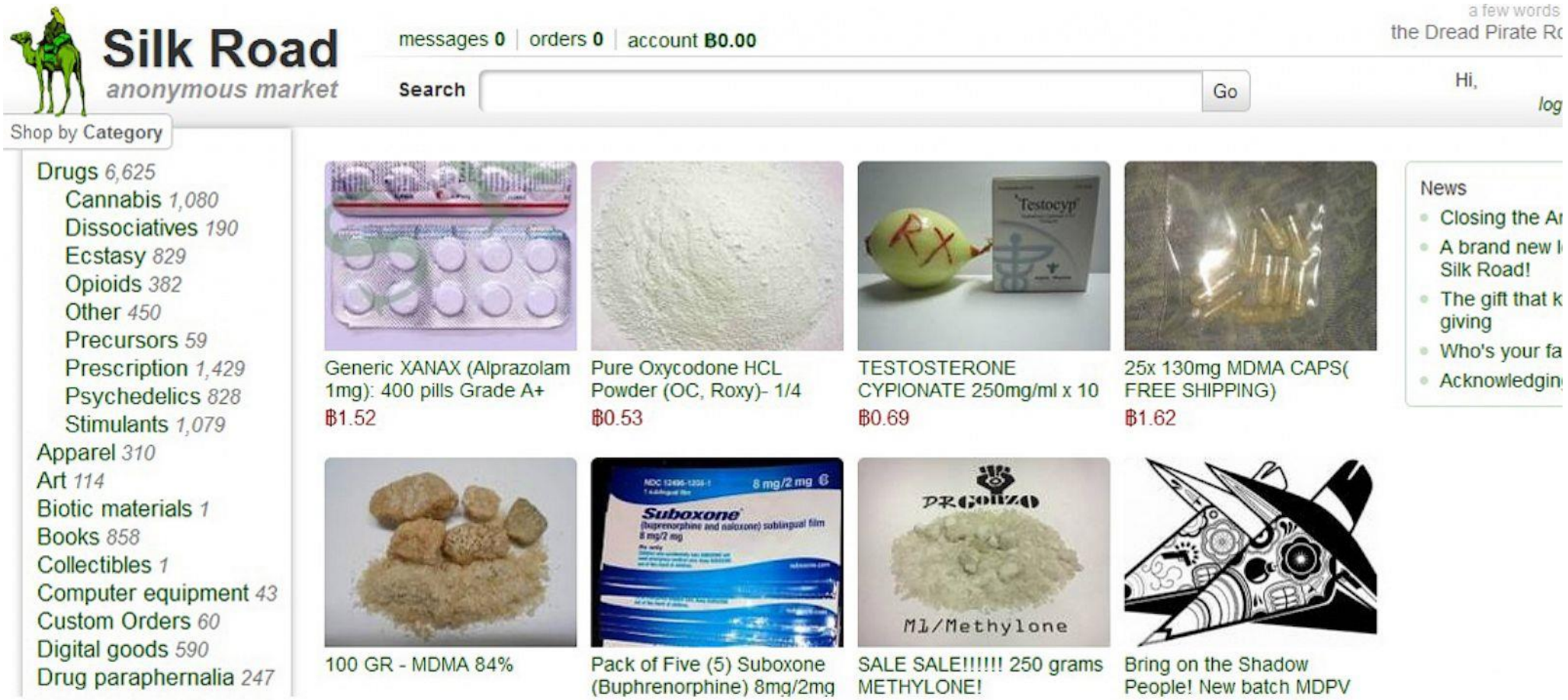
- ToR allows clients and relays to offer hidden services.
- Can offer a web server, SSH server, etc., without revealing your IP address to its users.
- ToR will generate a new public/private key pair for your hidden service. It is written into a file called "private_key".
- The other file ToR will create is called "hostname".
- This contains a short summary of your public key -- it will look something like **duskgytldkxiuqc6.onion**.
- This is the public name for your service, and you can tell it to people, publish it on websites, put it on business cards, etc.

TOR - BROWSER


About Tor
Tor Browser
Search or enter address
Search
New Identity ⌘⇧U
New Tor Circuit for this Site ⌘⇧L
Privacy and Security Settings…
Tor Network Settings…
Check for Tor Browser Update…
Tor Browser 6.0.6
Welcome to Tor Browser
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Search securely with Disconnect.me.
What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.
Tips On Staying Anonymous »
You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
Run a Tor Relay Node »
Volunteer Your Services »
Make a Donation »
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

ORBOT & ORFOX: TOR FOR ANDROID

REAL WORLD EXAMPLE



CONCLUSION

- TOR has long been used by Journalists, Researchers, or Thrill seekers in heavily censored countries in order to hide their web browsing habits and physical location, crawl the Deep Web and exchange information anonymously.
- One of the main reasons behind the rise of TOR is NSA's Surveillance Programs.
- 57% of the Dark Web is occupied by unauthorized contents like Pornography, Illicit Finances, Drug Hub, Weapon Trafficking, counterfeit currency flow and many more.
- Since internet traffic is being routed through at least three relays, it tends to get held up along the way.
- Dark Web is being defined as something that is illegal instead of a 'Pool of Information.'

REFERENCES

- https://turbofuture.com/internet/A-Beginners-Guide-to-Exploring-the-Darknet
- https://www.torproject.org/about/overview.html.en
- https://www.torproject.org/docs/hidden-services.html.en
- http://thehackernews.com/2016/02/deep-web-search-engine.html
- https://en.wikipedia.org/wiki/Tor_(anonymity_network)

REACH ME

- **E-Mail : svnair.adarsh@gmail.com**
- **Website : http://adarshnair.com**
- **LinkedIn : https://www.linkedin.com/in/adarshsvnair**
- **Facebook : https://www.facebook.com/adarshnair2018**
- **Twitter : https://twitter.com/adarshnair0406**


Thank you!