Cloud Native SECURITY DAY

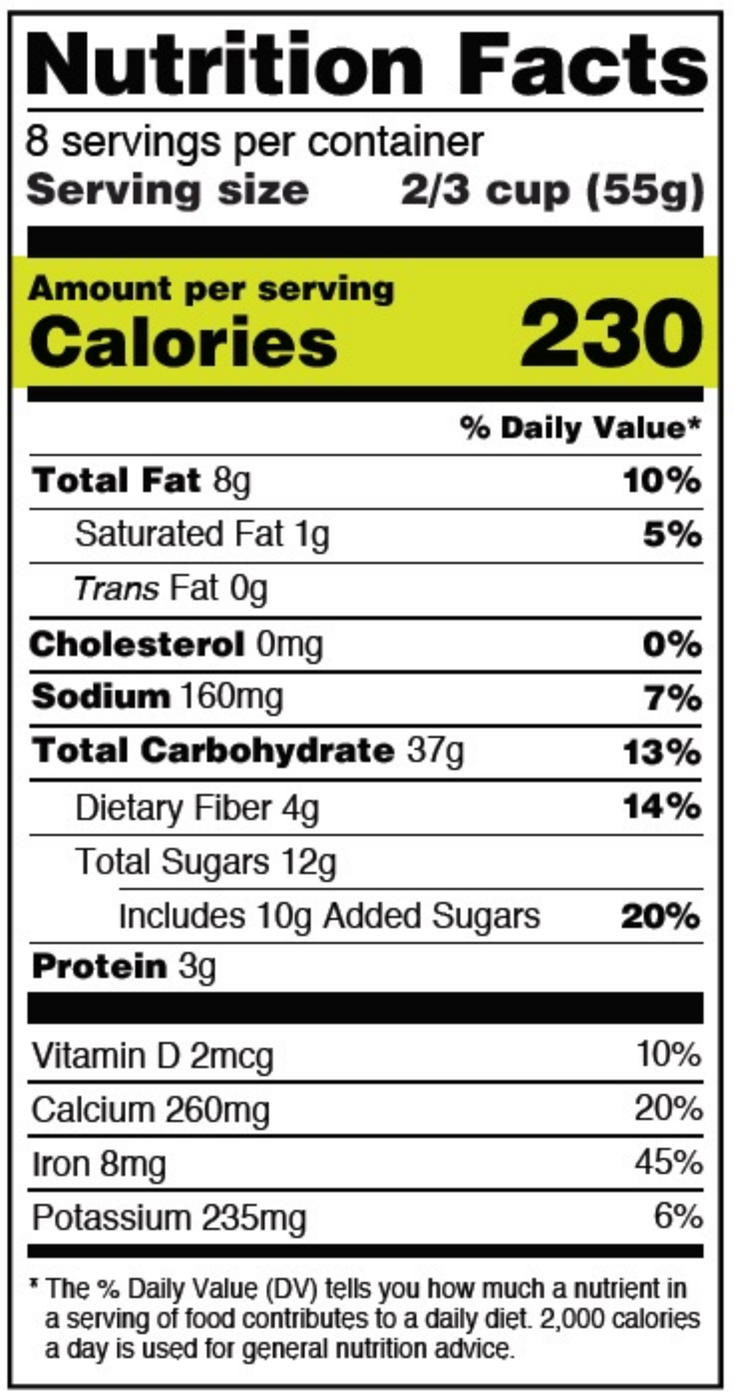
EUROPE

Cloud Native
SECURITY DAY
EUROPE

Security Nutrition Labels for Cloud Native Projects

John Kinsella

Nutrition label



Nutrition Facts

8 servings per container

Serving size **2/3 cup (55g)**

Amount per serving

Calories **230**

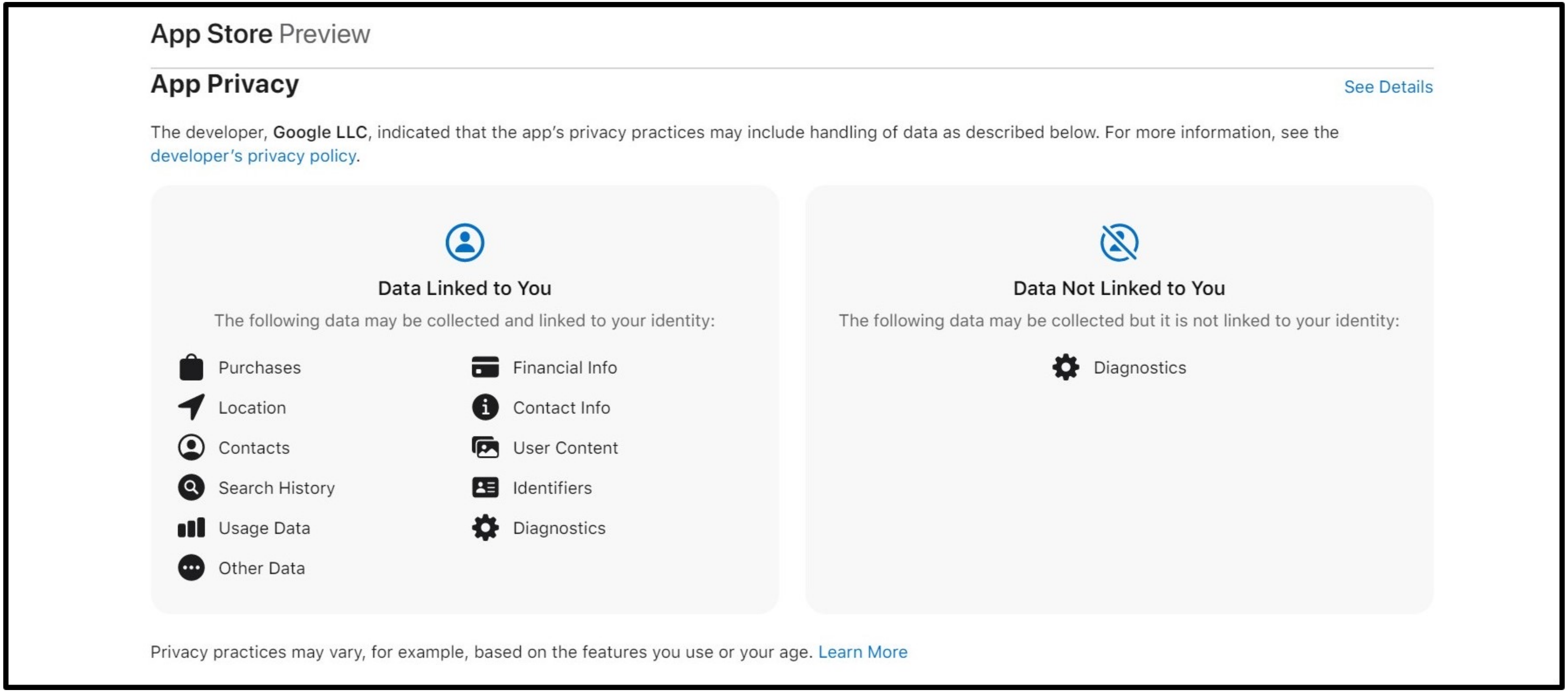
	% Daily Value*
Total Fat 8g	**10%**
Saturated Fat 1g	**5%**
Trans Fat 0g	
Cholesterol 0mg	**0%**
Sodium 160mg	**7%**
Total Carbohydrate 37g	**13%**
Dietary Fiber 4g	**14%**
Total Sugars 12g	
Includes 10g Added Sugars	**20%**
Protein 3g	
Vitamin D 2mcg	10%
Calcium 260mg	20%
Iron 8mg	45%
Potassium 235mg	6%

* The % Daily Value (DV) tells you how much a nutrient in a serving of food contributes to a daily diet. 2,000 calories a day is used for general nutrition advice.

History

- First nutrition laws created in early 1900s – just after packaged food
- 1970s – First labels mandated
- Tweaks to label requirements every decade or so

Apple App Store



App Store Preview

App Privacy

See Details

The developer, **Google LLC**, indicated that the app's privacy practices may include handling of data as described below. For more information, see the developer's privacy policy.

Data Linked to You

The following data may be collected and linked to your identity:

- Purchases
- Location
- Contacts
- Search History
- Usage Data
- Other Data
- Financial Info
- Contact Info
- User Content
- Identifiers
- Diagnostics

Data Not Linked to You

The following data may be collected but it is not linked to your identity:

- Diagnostics

Privacy practices may vary, for example, based on the features you use or your age. Learn More

Why is this needed?

- New to a project – is this something I can trust, or even use?

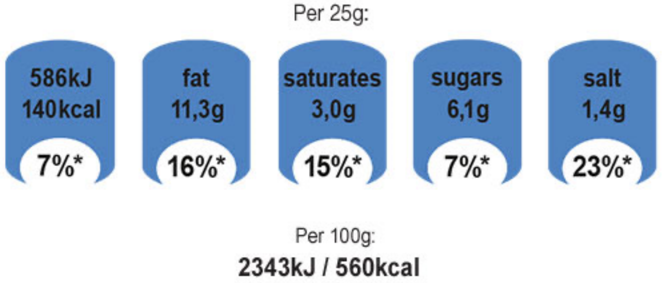
- Installation hell – every step has more requirements I didn’t know about

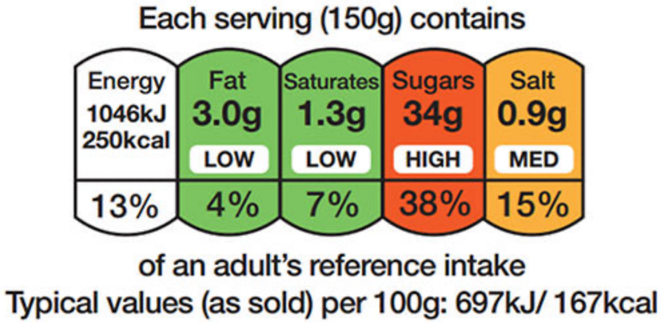
Security Label Goals

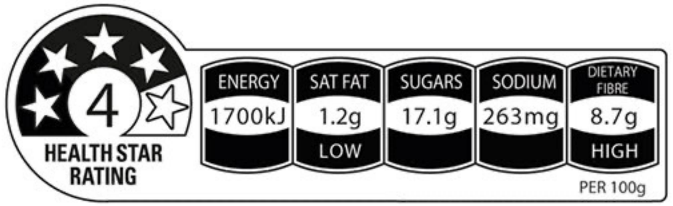
- Advise, not admonish
- Increase trust
- Increase default security posture

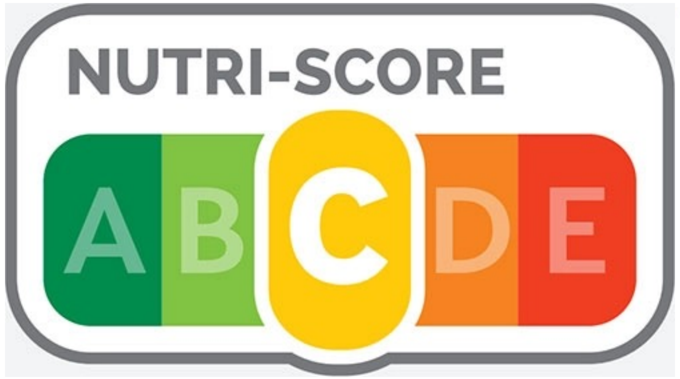
Front of Package Labels

Front of Package Labels



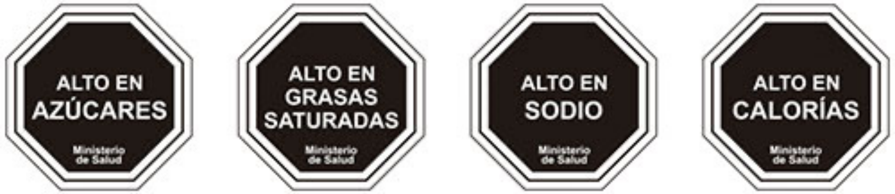

Each serving (150g) contains
Energy 1046kJ 250kcal
13%
Fat 3.0g LOW
4%
Saturates 1.3g LOW
7%
Sugars 34g HIGH
38%
Salt 0.9g MED
15%
of an adult's reference intake
Typical values (as sold) per 100g: 697kJ/ 167kcal





HEALTHY CHOICE ®
BASED ON INTERNATIONAL DIETARY GUIDELINES

HEALTHIER CHOICE
Health Promotion Board

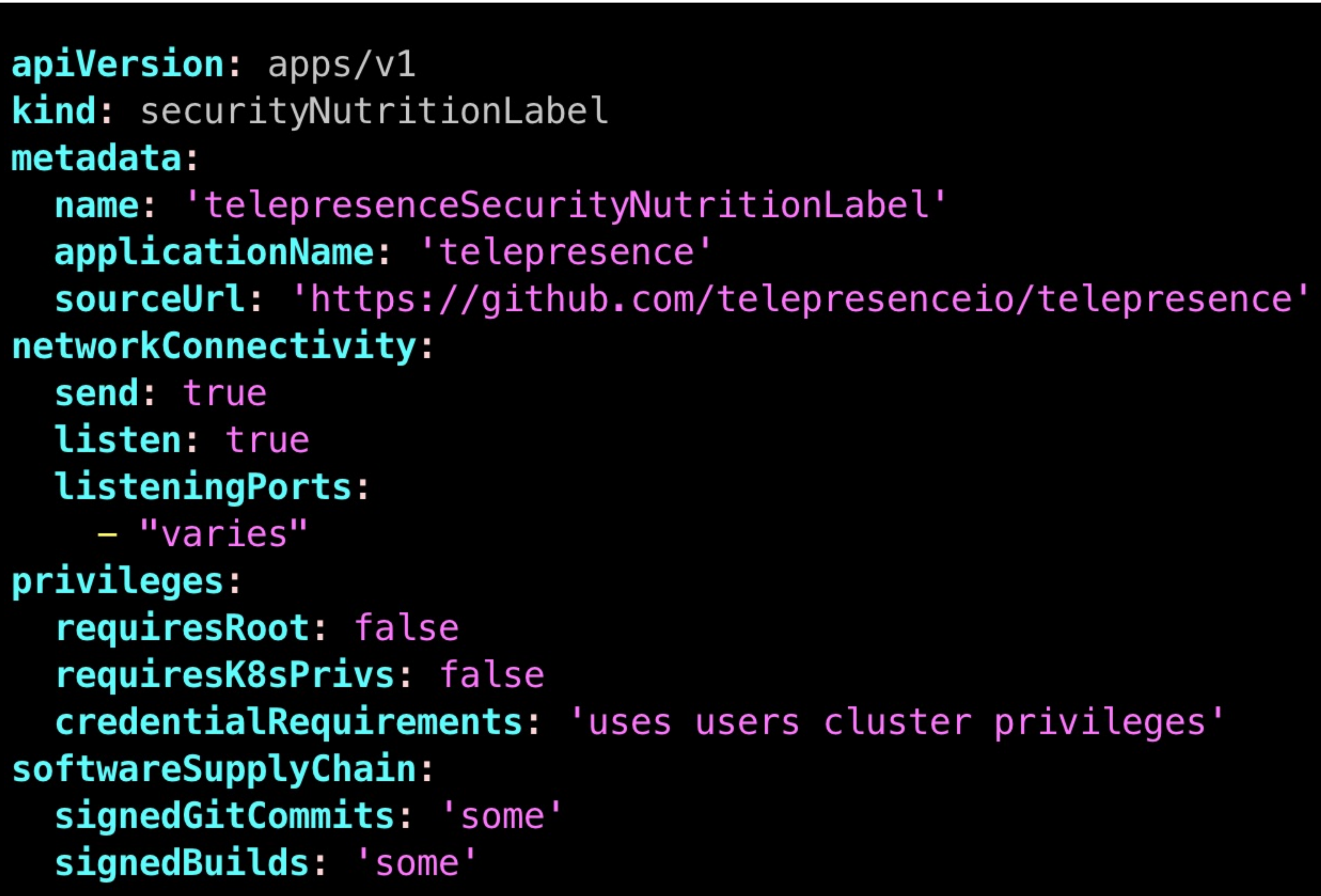


Label Contents

- Network connectivity – send or receive
- Root privileges required (cluster admin?)
- Credential requirements (CSP, k8s roles, API keys)
- Software supply chain status

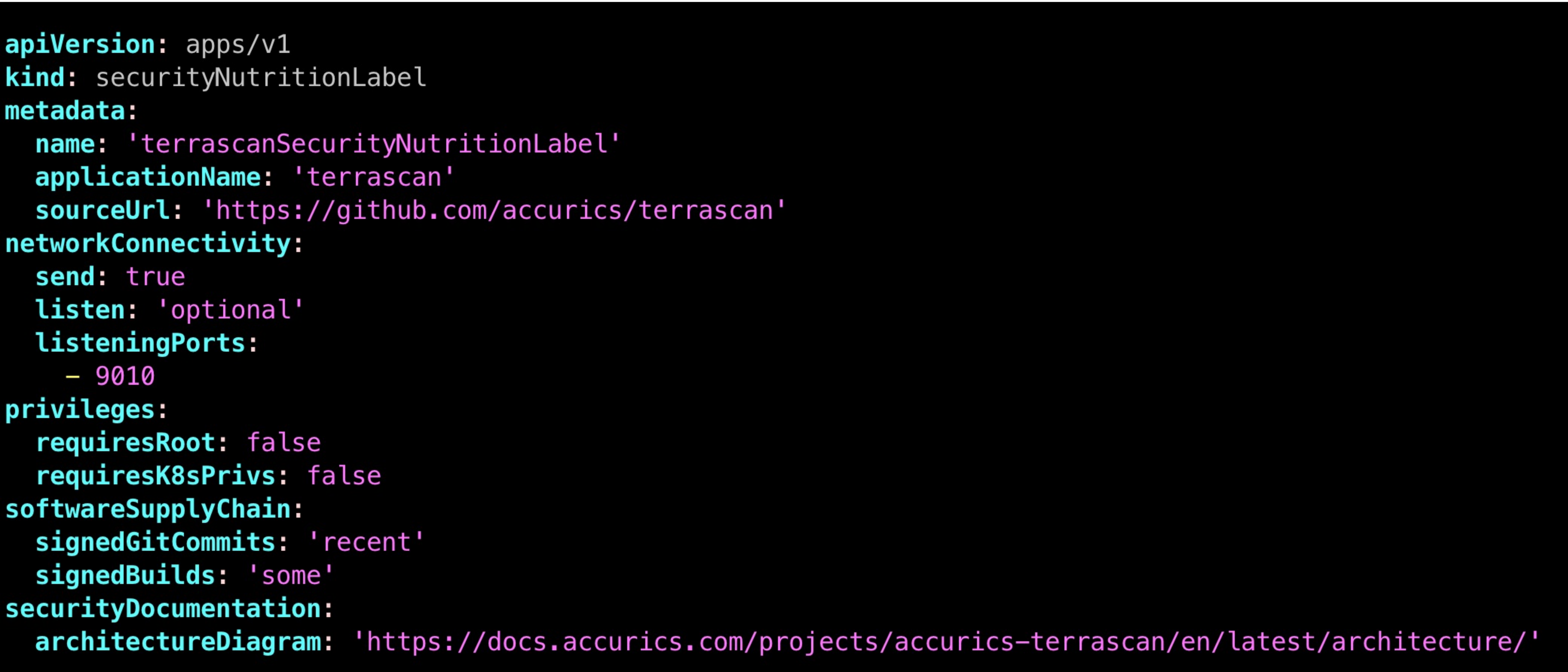
- Link to architecture diagram
- Link to threat model
- Link to self-assessment questionnaire
- Link to 3rd party review
- Security contact
- Security page

Example - telepresence



```
apiVersion: apps/v1
kind: securityNutritionLabel
metadata:
  name: 'telepresenceSecurityNutritionLabel'
  applicationName: 'telepresence'
  sourceUrl: 'https://github.com/telepresenceio/telepresence'
networkConnectivity:
  send: true
  listen: true
  listeningPorts:
    - "varies"
privileges:
  requiresRoot: false
  requiresK8sPrivs: false
  credentialRequirements: 'uses users cluster privileges'
softwareSupplyChain:
  signedGitCommits: 'some'
  signedBuilds: 'some'
```

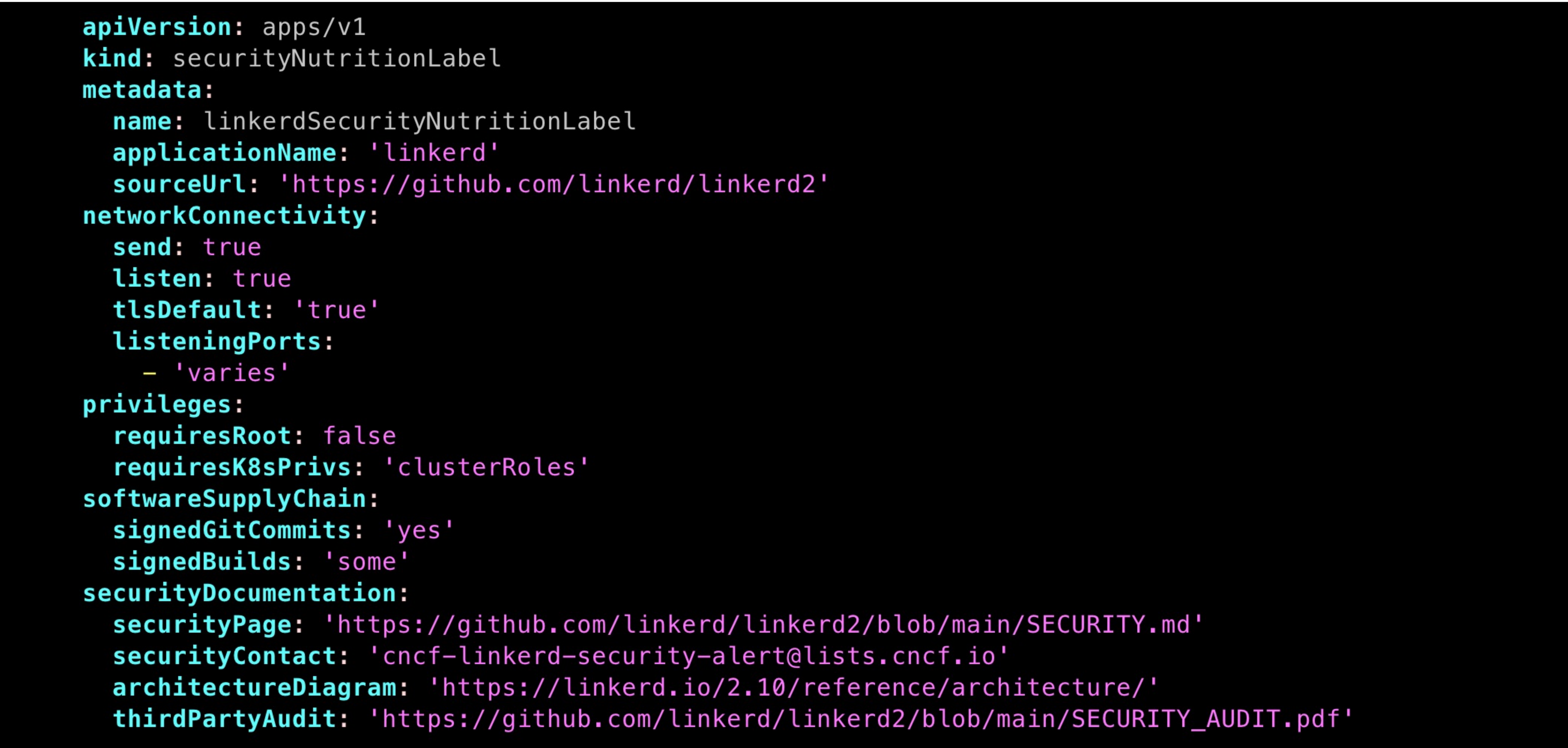
Example - terrascan



```yaml
apiVersion: apps/v1
kind: securityNutritionLabel
metadata:
  name: 'terrascanSecurityNutritionLabel'
  applicationName: 'terrascan'
  sourceUrl: 'https://github.com/accurics/terrascan'
networkConnectivity:
  send: true
  listen: 'optional'
  listeningPorts:
    - 9010
privileges:
  requiresRoot: false
  requiresK8sPrivs: false
softwareSupplyChain:
  signedGitCommits: 'recent'
  signedBuilds: 'some'
securityDocumentation:
  architectureDiagram: 'https://docs.accurics.com/projects/accurics-terrascan/en/latest/architecture/'
```

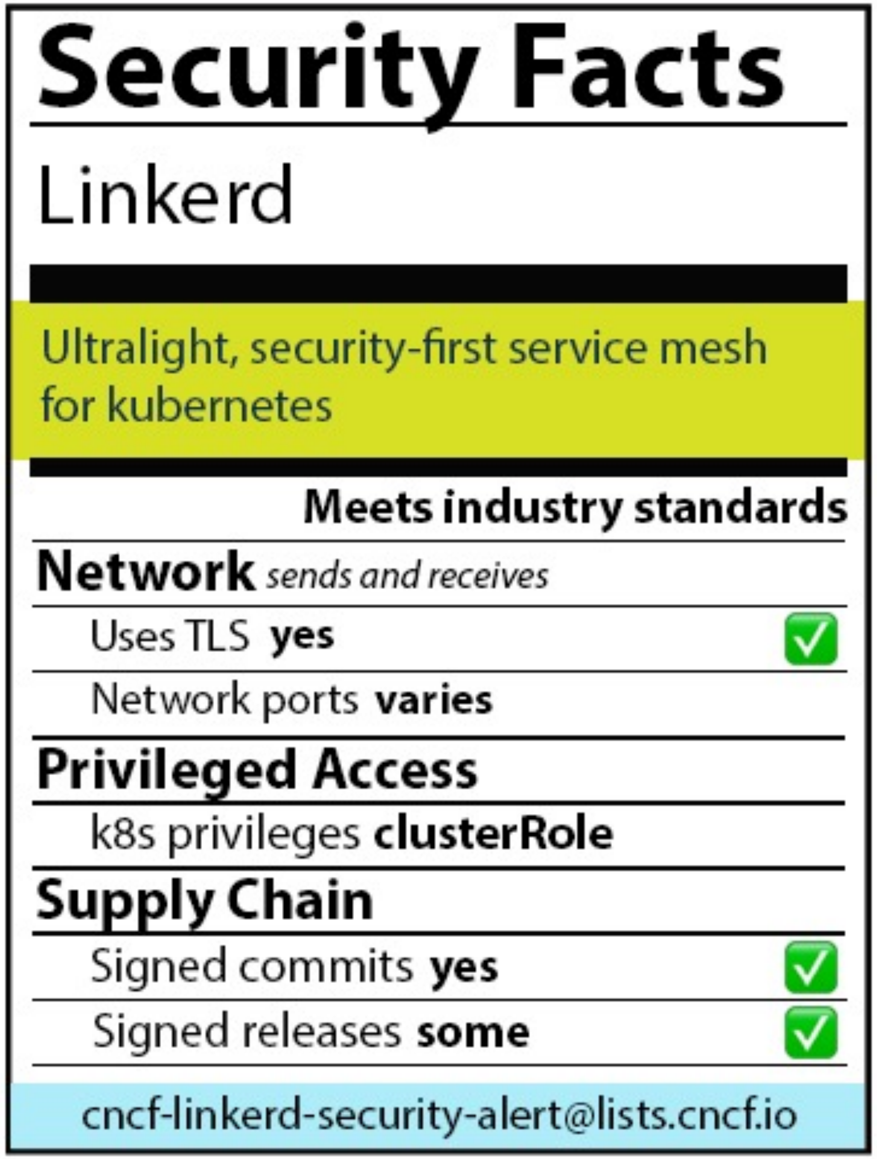
Example - linkerd

Cloud Native
SECURITY DAY
EUROPE



```yaml
apiVersion: apps/v1
kind: securityNutritionLabel
metadata:
  name: linkerdSecurityNutritionLabel
  applicationName: 'linkerd'
  sourceUrl: 'https://github.com/linkerd/linkerd2'
networkConnectivity:
  send: true
  listen: true
  tlsDefault: 'true'
  listeningPorts:
    - 'varies'
privileges:
  requiresRoot: false
  requiresK8sPrivs: 'clusterRoles'
softwareSupplyChain:
  signedGitCommits: 'yes'
  signedBuilds: 'some'
securityDocumentation:
  securityPage: 'https://github.com/linkerd/linkerd2/blob/main/SECURITY.md'
  securityContact: 'cncf-linkerd-security-alert@lists.cncf.io'
  architectureDiagram: 'https://linkerd.io/2.10/reference/architecture/'
  thirdPartyAudit: 'https://github.com/linkerd/linkerd2/blob/main/SECURITY_AUDIT.pdf'
```

Example - label



Security Facts

Linkerd

Ultralight, security-first service mesh for kubernetes

Meets industry standards

Network *sends and receives*

Uses TLS **yes** ✓

Network ports **varies**

Privileged Access

k8s privileges **clusterRole**

Supply Chain

Signed commits **yes** ✓

Signed releases **some** ✓

cncf-linkerd-security-alert@lists.cncf.io

Thanks!

Questions?

jlk on CNCF slack
@johnlkinsella on twitter

References

- https://www.fda.gov/food/new-nutrition-facts-label/calories-new-nutrition-facts-label
- https://apps.who.int/iris/bitstream/handle/10665/42964/9241591714.pdf
- https://www.igd.com/articles/article-viewer/t/front-of-pack-labelling-around-the-world/i/23126
- https://www.telepresence.io/
- https://cups.cs.cmu.edu/privacyLabel/files/CHI-finalPoster.pdf